



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DELIBERAÇÃO CGSIC/ IFS Nº 18, DE 30 DE JUNHO DE 2025

Aprova o Programa de Privacidade e  
Segurança da Informação (PPSI) do  
Instituto Federal de Sergipe - IFS.

**A PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE**, faz saber que, no uso das atribuições legais que lhe confere a Lei nº 11.892 de 29 de dezembro de 2008, em conformidade com a Portaria IFS nº 1.039 de 28/04/2014 e 1.339 de 05/06/2014, considerando a Portaria nº 1.038 de 27/04/2017 e a Norma Complementar nº 03/IN01/DSIC/GSIPR de 30/06/2009, e considerando a decisão proferida na 1ª Reunião Ordinária do Comitê Gestor Segurança de Informação e Comunicação em 2025 ocorrida em 27 de junho de 2025;

Resolve:

Art. 1º Aprovar o Programa de Privacidade e Segurança da Informação – PPSI do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe – IFS, na forma do anexo.

Art. 2º Esta deliberação entra em vigor no dia 1º de julho de 2025.

Aracaju, 30 de junho de 2025.

**Ruth Sales Gama de Andrade**  
Presidente do CGSIC/IFS



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

**PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO – PPSI**

**REFERÊNCIA LEGAL E DE BOAS PRÁTICAS**

- I. Constituição Federal de 1988;
- II. Norma ABNT NBR ISO/IEC nº 27001:2005 - Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerência da Segurança da Informação – Requisitos;
- III. Normas ABNT NBR ISO/IEC 27002:2005 – Técnicas de segurança – Código de práticas para a segurança da informação;
- IV. Normas ABNT NBR ISO/IEC 27003:2020 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Orientações;
- V. Norma ABNT NBR ISO nº 27017:2016 - Código de Práticas para a Gestão da Segurança da Informação;
- VI. Norma ABNT NBR ISO nº 27701:2019 - Técnicas de segurança para gestão da privacidade da informação – Requisitos e diretrizes.
- VII. Norma ISO/IEC TR nº 13335-3:1998, que fornece técnicas para a gestão de segurança na área de tecnologia da informação, baseada nas normas ISO/IEC nº 13335-1 e TR ISO/IEC nº 13335-2;
- VIII. Lei nº 7.232, de 29 de outubro de 1984, que dispõe sobre a Política Nacional de Informática;
- IX. Lei nº 8.112 de 11 de dezembro de 1990 - Regime jurídico dos servidores públicos civil da União, das autarquias e das fundações públicas federais;
- X. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;
- XI. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto Lei nº 2848/40 (Código Penal Brasileiro), de modo a prever a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
- XII. Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos;
- XIII. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- XIV. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais;
- XV. Decreto nº 1.171, de 24 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;
- XVI. 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;



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

XVII. 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;

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 8.771, 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;

XX. Decreto nº 9.573, de 22 de novembro de 2018, que aprova a Política Nacional de Segurança de Infraestruturas Críticas;

XXI. 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. Alterado pelo Decreto nº 9.832, de 12 de junho de 2019. Alterado pelo Decreto nº 10.641, de 2 de março de 2021;

XXII. Decreto nº 9.832, de 12 de junho de 2019, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação;

XXIII. Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

XXIV. Decreto nº 10.569, de 9 de dezembro de 2020, que aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas;

XXV. Decreto nº 10.641, de 2 de março de 2021, que altera o Decreto nº 9.637, de 26 de dezembro de 2018 e institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, altera o 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;

XXVI. Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos;

XXVII. Outros dispositivos legais aplicáveis, a saber:

a. Norma Complementar nº 01/IN01/DSIC/GSIPR, de 13 de outubro de 2008;

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



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

- c. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 3 de julho de 2009;
  - d. Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 de agosto de 2009;
  - e. Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
  - f. Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
  - g. Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos;
- XXVIII. Deliberação nº 01/2017/CGRC/IFS, de 31/01/2017. Aprova a Política de Gestão de Riscos e Controles Internos da Gestão do Instituto Federal de Sergipe (IFS);
- XXIX. Deliberação nº 63/2017/CGTIC/IFS, de 02/10/2017, Aprova Ad Referendum a Política de Governança de Tecnologia da Informação e Comunicação do Instituto Federal de Sergipe;
- XXX. Medida Provisória nº 1.124, de 13 de junho de 2022. Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão;
- XXXI. Instrução Normativa SGD nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- XXXII. Instrução Normativa SGD nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;
- XXXIII. Instrução Normativa SGD nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;
- XXXIV. Instrução Normativa SGD nº 117, de 19 de novembro de 2020, que dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;
- XXXV. Portaria GSI nº 38, de 14 de agosto de 2009, que homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR - Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;
- XXXVI. Portaria GSI nº 40, de 8 de outubro de 2014, que homologa a Norma Complementar nº 21/IN01/DSIC/GSIPR - Estabelece Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta;
- XXXVII. Portaria GSI nº 57, de 23 de agosto de 2010, que homologa a Norma Complementar nº 08/IN01/DSIC/GSIPR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais - Gestão de ETIR, nos órgãos e entidades da Administração Pública Federal;



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

XXXVIII. Portaria GSI nº 93, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação.



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

**PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)**

**CAPÍTULO I**

**DAS DISPOSIÇÕES PRELIMINARES**

Art. 1º A informação é um ativo que a organização tem o dever e a responsabilidade de proteger. A disponibilidade da informação de forma completa e precisa é essencial para que a organização forneça de forma eficiente os serviços.

Art. 2º A proposta deste Programa de Privacidade e Segurança da Informação (PPSI) é estabelecer as diretrizes para a proteção dos ativos de informação do IFS. Esse documento contém diretrizes gerais de segurança e controle de proteção da informação. Tais controles são descritos e padronizados pelos processos e procedimentos de segurança da informação com ferramentas e conscientizações.

Art. 3º A política visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de dados pessoais (LGPD) e outra normas vigentes. Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos usuários, quando na utilização dos recursos de processamento da informação do IFS.

**Seção I**

**Do Objetivo e Metas**

Art. 4º Regularizar e normatizar o uso dos recursos e serviços prestados pelos setores de Tecnologia da Informação (TI) da Reitoria e de todos os campi da instituição, visando atingir as seguintes metas:

- a) Melhoria da segurança dos usuários online;
- b) Melhorias da segurança dos meios de comunicação de dados;
- c) Melhoria da segurança dos sistemas computacionais;
- d) Mitigação de riscos à segurança da informação;
- e) Normatizar a proteção de dados pessoais.

**Seção II**

**Do Escopo e abrangência**

Art. 5º O PPSI se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações do IFS. Este programa se aplica em todas as instalações físicas administradas ou utilizadas pelo IFS e entidades subsidiárias.



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 6º O escopo da Política de Segurança da Informação (PSI) do IFS refere-se:

- a) Aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que os incorporarão;
- b) Aos requisitos de segurança humana;
- c) Aos requisitos de segurança física;
- d) Aos requisitos de segurança lógica;
- e) À sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços oriundos da informação e comunicação do IFS.

### Seção III

#### Dos termos e definições

Art.7º Para os efeitos deste Programa são estabelecidos os seguintes termos e definições:

- I. Agentes de tratamento: o controlador e o operador;
- II. Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição, nos termos da Norma ISO/IEC nº 13335-1:2004;
- III. Análise de riscos: uso sistemático de informações para identificar fontes e estimar seu risco;
- IV. Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- V. Ativo de informação: qualquer informação que tenha valor para a Instituição, nos termos da Norma ISO/IEC nº 13335-1:2004;
- VI. Avaliação de riscos: processo por intermédio do qual se compara o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;
- VII. Comunicação oficial: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IFS, de atividades especiais ou ainda de projetos específicos;
- VIII. Comunicação informal: tráfego de documentos, informações ou formulários que não sejam incluídos no conceito de que trata o inciso anterior, emitidos via caixas postais eletrônicas individuais de autoridade, servidor, estagiário ou fornecedor de bens e/ou serviços;
- IX. Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- X. Contingência: indisponibilidade ou perda de integridade da informação que os controles de segurança não tenham conseguido evitar;



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

- XI. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- XII. 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;
- XIII. Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- XIV. Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- XV. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- XVI. Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- XVII. 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;
- XVIII. Gestão de Riscos de Segurança da Informação e Comunicação: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias, especificamente, para mitigar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;
- XIX. Gestor: agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas de uso da informação;
- XX. Identificação de riscos: processo de localização, enumeração e caracterização dos elementos do risco;
- XXI. Incidente de segurança da informação: ocorrência indicada por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que apresentem grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação, nos termos da Norma ISO/IEC TR nº 18044:2004;
- XXII. Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- XXIII. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

XXIV. Plano de continuidade de negócios: conjunto de procedimentos a serem adotados quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços;

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

XXVI. Políticas de Segurança da Informação (PSI) - Documento aprovado pela autoridade máxima do órgão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficiente à implementação da segurança da informação e comunicação;

XXVII. Princípios da Segurança da Informação e Comunicação: princípios que regem a Segurança da Informação e Comunicação, nos termos do art. 3º do Decreto nº 3.505, de 13 de junho de 2000, ou seja, a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio;

XXVIII. Programa de Privacidade e Segurança da Informação (PPSI) - Caracteriza-se como um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação, com o objetivo de elevar a maturidade e a resiliência do IFS, em termos de privacidade e segurança da informação;

XXIX. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulte no comprometimento da Segurança da Informação e Comunicação;

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

XXXI. Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXII. Titular do dado: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XXXIII. Termo de responsabilidade: acordo de confidencialidade e não divulgação de informações, que atribui responsabilidades ao servidor e ao administrador de serviço quanto ao sigilo e à correta utilização dos ativos de propriedade da Instituição ou por ela custodiados;

XXXIV. Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

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

XXXVI. Tratamento dos riscos: processo de implementação de ações de Segurança da Informação e Comunicações destinadas a evitar, reduzir, reter ou transferir um risco;



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

XXXVII. Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XXXVIII. Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e/ou equipamentos que não esteja vinculada administrativamente ao IFS;

XXXIX. Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e/ou equipamentos que estejam vinculados administrativamente ao do IFS;

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

**CAPÍTULO II**  
**DOS PRINCÍPIOS**

Art.8º As ações de segurança da informação do IFS são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

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

II. Integridade: somente operações de alteração, supressão e adição autorizadas pelo IFS devem ser realizadas nas informações;

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

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

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

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

VII. 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 IFS são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação advindas desta Política;



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

VIII. 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;

IX. Ética: todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFS devem ser respeitados;

X. Legalidade: além de observar os interesses do IFS, 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 aos direitos de uso;

XI. Proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no âmbito IFS serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

**CAPÍTULO III**  
**DAS DIRETRIZES GERAIS**

Art.9º As diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito desta entidade e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos neste programa.

Art. 10 Cada servidor público é responsável pela Segurança da Informação dentro do IFS, principalmente pelas informações que estão sob sua responsabilidade.

Art. 11 O IFS, como usuário dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança.

Art. 12 Os usuários internos e externos devem observar que:

I. O acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFS é considerada seu patrimônio e deve ser protegida;

II. Os recursos disponibilizados pelo IFS, e de sua propriedade, são fornecidos com o propósito único de garantir o desempenho das suas atividades;

III. As normas para as operações de armazenamento, divulgação, reprodução, recuperação e destruição da informação serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor.

Art. 13 Tratamento da Informação - A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do IFS. Essa proteção deve ser de acordo com o valor, sensibilidade e criticidade da informação, devendo ser desenvolvido, para este fim, sistema de



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

classificação da informação. Os dados, as informações e os sistemas de informação do IFS devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Art. 14 Gestão de Incidentes - Será estabelecido um serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências.

Art. 15 Gestão de Riscos - Será estabelecido um processo de Gestão de Riscos, contínuo e aplicado na implementação e operação da Gestão de Segurança de Informação e Comunicação, produzindo subsídios para a Gestão de Continuidade dos Negócios. Os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco, como ameaça, vulnerabilidade, probabilidade e impacto.

Art. 16 Auditoria e Conformidade - Deverá ser levantado regulamente os aspectos legais de segurança aos quais as atividades do IFS estão submetidas de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão.

Art. 17 Controles de acesso - Controles que monitoram o acesso físico a equipamentos, documentos, suprimentos e locais físicos do IFS e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança.

Art.18 Uso de e-mail - O serviço de correio eletrônico disponibilizado pelo IFS constitui recurso do Instituto disponibilizado na rede de comunicação de dados para aumentar a agilidade, segurança e economia da comunicação oficial e informal. O correio eletrônico constitui bem do IFS e, portanto, é passível de auditoria;

Art. 19 Acesso à Internet - O acesso à Internet será concedido para todos os servidores, com utilização exclusiva para fins diretos e complementares às atividades do setor. O acesso à Internet será concedido para todos os alunos com utilização para fins acadêmicos e/ou atividades que não infrinjam a este PPSI. Todo acesso à Internet será monitorado e passível de auditoria.

Art. 20 Termo de Responsabilidade e Sigilo - É o documento oficial que compromete colaboradores, terceirizados e prestadores de serviços com o PPSI do IFS, os quais deverão ser signatários.

Art. 21 Gestão da Continuidade - Para assegurar a disponibilidade e, conseqüentemente, a continuidade dos serviços e recursos providos na infraestrutura de TI do IFS, deve-se; (a) planejar ações de prevenção e recuperação; (b) determinar prazos máximos de recuperação de sistemas de acordo com a criticidade dos processos envolvidos. Isso poderá manter os serviços disponíveis ou mesmo reduzir os impactos decorrentes da interrupção deles, sob a ocorrência de desastres ou falhas de segurança.

Art. 22 Desenvolvimento de software – As normas para o desenvolvimento de softwares seguros no IFS serão regulamentadas por normas complementares específicas, em conformidade com a norma do DSIC 16/IN01/DSIC/GSIPR, que complementarará esta política de segurança.



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

**CAPÍTULO IV**

**DA ESTRUTURA NORMATIVA DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)**

Art. 23 A estrutura normativa da Segurança da Informação do IFS é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

I. Política de Segurança da Informação (Política): Constituída por este documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação e Comunicação, e será detalhada em um conjunto de Normas específicas;

II. Normas de Segurança da Informação (Normas): Estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem observados em diversas instâncias em que a informação seja tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas no documento “Atividade de Normatização” do Departamento de Segurança da Informação e Comunicações do gabinete de Segurança Institucional da Presidência da República;

III. Procedimentos de Segurança da Informação e Comunicação (Procedimentos): Instrumentalizam o disposto nas Normas, permitindo sua direta aplicação nas atividades do IFS, cabendo a cada gestor a responsabilidade de gerá-los. Cada procedimento poderá ainda ser detalhado em instruções. Estes procedimentos e instruções serão de uso interno, não sendo obrigada a sua publicação.

**CAPÍTULO V**

**DAS INSTÂNCIAS ADMINISTRATIVAS**

Art. 24 Para os efeitos desta política e das normas nela originadas, entende-se por:

I. Comitê Gestor de Segurança da Informação e Comunicação (CGSIC): comitê responsável por elaborar e revisar periodicamente o programa de Privacidade e Segurança da Informação (PPSI) e normas relacionadas, entre outras competências.

II. Diretoria de Tecnologia da Informação (DTI): órgão executivo, que planeja, dirige, avalia e executa as políticas de Tecnologia da Informação e Comunicação (TIC) em todo o Instituto, em articulação com as Pró-Reitorias e as Direções Gerais dos Campi.

III. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

IV. Gestor de Segurança da Informação e Comunicação: responsável pelas ações de segurança da informação e comunicação no âmbito do IFS.



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

CAPÍTULO VI  
DAS RESPONSABILIDADES E COMPETÊNCIAS

Art. 25 A responsabilidade pela segurança das informações deverá estar estabelecida nos documentos oficiais do IFS e principalmente na Política de Segurança da Informação (PSI).

Art. 26 O monitoramento do uso da internet é importante para que sejam registrados todos os acessos de cada usuário e para que possam ser notificados e até mesmo punidos nos casos de acesso que sejam contrários a política do IFS.

Art. 27 São responsabilidades dos usuários de serviços de redes de dados, internet, correio eletrônico e/ou outros recursos computacionais oferecidos pelo IFS:

- I. Promover a segurança do seu usuário corporativo, bem como suas respectivas senhas;
- II. A identificação do usuário por meio de senha é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas com o uso dela;
- III. Seguir de forma colaborativa as orientações fornecidas pelos setores competentes em relação ao melhor uso dos recursos computacionais, de rede de dados, internet, telecomunicações e correio;
- IV. Utilizar de forma ética e legal os recursos computacionais, de rede de dados, internet, telecomunicações e correio eletrônico.

Art. 28 Compete à Diretoria de Tecnologia da Informação zelar pela segurança da informação no âmbito do IFS quando as informações estiverem sob custódia dos recursos de tecnologia da informação.

Art. 29 Compete aos Setores de Tecnologia da Informação dos campi zelar pela segurança da informação no âmbito de cada campus quando as informações estiverem sob custódia dos recursos de tecnologia da informação.

Art. 30 Ao Comitê Gestor de Segurança da Informação e Comunicação compete:

- I. Promover a cultura de Segurança da Informação;
- II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- III. Propor recursos necessários às ações de Segurança da Informação;
- IV. Realizar e acompanhar estudos de novas tecnologias, no que diz respeito a possíveis impactos sobre a Segurança da Informação;
- V. Coordenar as revisões das normas de segurança em vigor;
- VI. Fazer trabalho de conscientização, educação e treinamento da segurança da informação no âmbito do IFS;



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

- VII. Acordar sobre papéis e responsabilidades específicas para segurança de informações em toda a organização;
- VIII. Acordar sobre metodologias e processos específicos para segurança de informações;
- IX. Apoiar iniciativas de segurança de informação que abrangem toda a organização. Por exemplo: programas de conscientização sobre segurança;
- X. Promover a visibilidade do suporte corporativo para a segurança de informações em toda a organização.
- XI. Aprovar o PPSI.

#### CAPÍTULO VII

#### DA DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

Art. 31 A alta direção IFS, na figura do(a) Reitor(a), declara-se comprometida em proteger todos os seus ativos de informação.

#### CAPÍTULO VIII

#### DAS VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 32 O não cumprimento das determinações do PPSI sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do IFS.

Art. 33 O descumprimento das disposições constantes no Programa, Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 34 O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente.

#### CAPÍTULO IX

#### DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Art. 35 O Programa, Política e as Normas de Segurança da Informação e Comunicação devem ser divulgados a todos os servidores do IFS, e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.



**MINISTÉRIO DA EDUCAÇÃO**  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE  
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

§1º As áreas atingidas por este PPSI são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento.

§2º As áreas deverão submeter suas propostas de normas ao “Comitê de Segurança da Informação e Comunicação” para análise, discussão e aprovação no âmbito do Comitê;

§3º Após aprovação, estas normas e procedimentos serão divulgadas aos interessados pela área responsável por sua proposição e manutenção.

**CAPÍTULO X**  
**DA REVISÃO E ATUALIZAÇÃO**

Art. 36 O programa PODERÁ ser atualizado sempre que uma nova tecnologia surgir, instruções normativas existentes sofrerem alterações ou conforme necessidade do CGSIC. Deverá ser revisada anualmente ou conforme necessidade do CGSIC.