



SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO
REITORIA

**RESOLUÇÃO Nº 29 DO CONSELHO SUPERIOR,
DE 29 DE SETEMBRO DE 2026.**

Aprova a Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - IF SERTÃO-PE.

O Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, no uso de suas atribuições legais, conforme designação estabelecida pelo Decreto Presidencial de 16 de maio de 2024, publicado no Diário Oficial da União (D.O.U.) nº 95, de 17 de maio de 2024, Seção 2, RESOLVE:

Art. 1º APROVAR a Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - IF SERTÃO-PE.

Art. 2º REVOGA a Resolução nº 24, de 10 de agosto de 2020.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Documento assinado digitalmente
gov.br JEAN CARLOS COELHO DE ALENCAR
Data: 02/10/2026 10:37:47-0300
Verifique em <https://validar.iti.gov.br>

Jean Carlos Coelho de Alencar
Presidente do Conselho Superior

PUBLICADO NO SITE INSTITUCIONAL EM: 29/09/2026.



INSTITUTO FEDERAL
Sertão Pernambucano

Política de Segurança da Informação (PSI)

Instituto Federal de Educação,
Ciência e Tecnologia do
Sertão Pernambucano

Setembro
2026



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DO SERTÃO PERNAMBUCANO

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Descrição	Autor
1.0	20/11/2025	Elaboração da Política de Segurança da Informação	Equipe Técnica de Elaboração
1.1	17/12/2025	Revisão	Francisco Hamilton
1.2	15/09/2026	Revisão	Conselho Dirigente
1.3	18/09/2026	Revisão e ajustes	Câmara de Desenvolvimento Institucional
1.4	25/09/2026	Aprovação	Conselho Superior

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Esta Política de Segurança da Informação (PSI) está em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), com o Programa de Privacidade e Segurança da Informação (PPSI) e com a Política de Governança Digital. Com isso, esta PSI se aplica aos seguintes grupos do Instituto Federal de Educação, Ciência e Tecnologia de Sertão Pernambucano (IFSertãoPE):

- I. todos os servidores, sejam servidores efetivos ou temporários, do IFSertãoPE;
- II. todos os contratados e terceiros que prestam serviços para o IFSertãoPE;
- III. todos os colaboradores externos; e
- IV. todos os discentes e visitantes.

Art. 2º Esta Política de Segurança da Informação refere-se:

- I. aos aspectos estratégicos, estruturais, bem como os organizacionais;
- II. aos requisitos da segurança física de tecnologia da informação; e
- III. aos requisitos da segurança lógica.

Art. 3º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo IFSertãoPE devem estar em conformidade com esta Política de Segurança da Informação.

CAPÍTULO II

DOS PRINCÍPIOS E OBJETIVOS

Art. 4º O objetivo desta Política de Segurança da Informação é estabelecer princípios, diretrizes e responsabilidades para garantir a proteção das informações institucionais físicas e digitais do Instituto Federal de Educação, Ciência e Tecnologia de Sertão Pernambucano (IFSertãoPE), assegurando a confidencialidade, integridade, disponibilidade, autenticidade e conformidade legal.

Art. 5º. As ações de segurança da informação do IFSertãoPE são orientadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

- I. disponibilidade, integridade, confidencialidade e autenticidade das informações;
- II. continuidade dos processos e serviços essenciais para o funcionamento do IFSertãoPE;
- III. economicidade da proteção dos ativos de informação;
- IV. respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;
- V. observância da publicidade como preceito geral e do sigilo como exceção;
- VI. responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;
- VII. alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do IFSertãoPE, assim como demais normas específicas de segurança da informação da Administração Pública Federal;
- VIII. conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis; e
- IX. educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 6º. Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito do IFSertãoPE e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º. As normas, procedimentos, manuais e metodologias de segurança da informação do IFSertãoPE devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º. As ações de segurança da informação devem:

- I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do IFSertãoPE;
- II. ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do IFSertãoPE;
- III. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e
- IV. visar à prevenção da ocorrência de incidentes.

Art. 9º. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao IFSertãoPE.

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no IFSertãoPE compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Art. 11 A Política de Segurança da Informação e suas atualizações, bem como as normas específicas de segurança da informação do IFSertãoPE, devem ser divulgadas amplamente a todos os usuários de informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º O IFSertãoPE promoverá ações contínuas de capacitação e conscientização dos usuários de informação nos procedimentos de segurança e no uso correto dos ativos, cabendo aos usuários participar das capacitações disponibilizadas para a correta realização de suas atribuições e minimização de riscos.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 12 Para os efeitos desta Política de Segurança da Informação, aplicam-se os seguintes conceitos e definições:

I - ANPD: acrônimo de Agência Nacional de Proteção de Dados.

II - Ativo de Informação: Ativo associado ao processamento, armazenamento ou transmissão de informações que tem valor reconhecido para a organização como, por exemplo, dados, equipamentos (hardwares), softwares, serviços de TI, pessoas, infraestrutura e instalações.

III - Autenticação Multifator (MFA): *Multifactor Authentication* (MFA) é a utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito).

IV - Backup ou Cópia de Segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de perda das originais. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

V - Conscientização: atividade que tem por finalidade orientar sobre o que é SI levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros.

VI - Controlador: Pessoa natural ou jurídica, autoridade pública, agência ou outro organismo que determina as finalidades e os meios do tratamento de dados pessoais.

VII - Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados.

VIII - ETIR: acrônimo para Equipe de Prevenção, Tratamento e Resposta à Incidentes Cibernéticos, ou seja, grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

IX - Gestão de Riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

X - Hypertext Transfer Protocol Secure (HTTPS): extensão do HTTP utilizada para comunicação segura pela rede de computadores. No HTTPS, o protocolo de comunicação é criptografado usando o TLS ou o seu predecessor, o SSL. A principal motivação para o uso do HTTPS é a autenticação do site acessado e a proteção da privacidade e integridade dos dados trocados durante o tráfego de informações.

XI - Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

XII - Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

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

XIV - Infraestrutura Crítica: instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocaram sério impacto social, econômico, político, internacional ou à segurança.

XV - LGPD: acrônimo de Lei Geral de Proteção de Dados Pessoais.

XVI - Risco de Segurança da Informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

XVII - SSH (Secure Shell): protocolo de rede criptográfico utilizado para permitir a comunicação segura e o gerenciamento remoto de sistemas operacionais, como servidores. Ele fornece um método seguro para acessar e operar um computador por meio de uma rede não segura, substituindo protocolos inseguros como o Telnet e o FTP.

XVIII - Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externas à organização.

XIX - Titulares de dados pessoais: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

XX - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

XXI - Tratamento da Informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.

CAPÍTULO IV

DA ESTRUTURA NORMATIVA

Art. 13 A estrutura normativa da Segurança da Informação do IFSertãoPE 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, devendo esta ser publicada por meio de Portaria;

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. Devendo esta ser publicada por meio de Instrução Normativa; e

III. **Procedimentos de Segurança da Informação:** instrumentalizam o disposto nas normas, permitindo sua direta aplicação no âmbito do IFSertãoPE. Devendo esta ser publicada na forma de documentação interna.

CAPÍTULO V

DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 14 A estrutura de Gestão de Segurança da Informação deverá ser composta por:

1. Reitor do IFSertãoPE;
2. Comitê Gestor de Segurança da Informação;
3. Comitê de Governança Digital;

4. Comitê Gestor de Tratamento de Dados Pessoais;
5. Diretoria de Gestão de Tecnologia da Informação:
 1. Coordenação de Infraestrutura de Redes e Segurança;
 1. Setor de Serviços e Suporte em TI;
 2. Setor de Segurança da Informação
 2. Setor de Governança em Tecnologia da Informação;
 3. Coordenação de Gestão e Desenvolvimento de Sistemas da Informação.

CAPÍTULO VI

DIRETRIZES

Seção I

Inventário de Ativos

Art. 15 O IFSertãoPE deverá registrar, estabelecer e manter um inventário dos ativos de informação institucionais (incluindo *hardware*, *software*, bases de dados, documentos físicos críticos e infraestrutura), garantindo o mapeamento daqueles que armazenam, processam ou transmitem dados e informações.

Parágrafo único. Seus registros devem conter informações precisas e detalhadas dos ativos, possibilitando sua identificação, classificação de criticidade e rastreabilidade.

Art. 16 Os ativos tecnológicos ou físicos não autorizados conectados à rede ou presentes nas dependências do IFSertãoPE deverão ser identificados e gerenciados para mitigar riscos à segurança da informação.

Art. 17 A identificação e a classificação dos ativos críticos do IFSertãoPE, incluindo infraestruturas de *datacenters*, repositórios corporativos e serviços em nuvem, deverão ser priorizadas no mapeamento e no inventário de ativos.

Art. 18 O IFSertãoPE estabelecerá critérios para classificar a criticidade dos ativos de informação, de modo a orientar a priorização das medidas de proteção e a gestão de riscos descritas nesta Política.

Art. 19 Os *softwares* e sistemas operacionais homologados para uso no ambiente institucional devem possuir suporte ativo de seus desenvolvedores ou mantenedores para garantia de atualizações de segurança.

Parágrafo único. Casos excepcionais ou sistemas legados incapazes de receber suporte ativo deverão ser registrados no inventário de ativos acompanhados da devida análise de risco e das medidas mitigadoras adotadas, observado o disposto no art. 76 desta Política.

Seção II

Riscos de Segurança da Informação

Art. 20 Deverá ser estabelecida uma Gestão de Riscos de Segurança da Informação (GRSI) com vistas a minimizar possíveis impactos associados aos ativos de informação, possibilitando a seleção e a priorização dos ativos de informação a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

Art. 21 O IFSertãoPE, conforme a GRSI, irá dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo de informação que está sendo protegido e de acordo com a identificação de riscos de potenciais prejuízos ao negócio, à atividade fim e aos objetivos institucionais.

Seção III

Proteção de Dados

Art. 22 O IFSertãoPE deverá criar, estabelecer e manter um processo de gestão de dados que trate dos seguintes aspectos:

- I. sensibilidade dos dados;
- II. proprietário;
- III. manuseio;
- IV. limites de retenção; e
- V. requisitos de descarte.

Art. 23 O descarte de dados (físico ou lógico) deve ser realizado de forma segura, garantindo que não seja recuperável.

Art. 24 O uso de criptografia para dispositivos de usuários que possuam dados sensíveis e/ou confidenciais deve ser implementado, onde for suportado.

Seção IV Configuração Segura

Art. 25 O IFSertãoPE deve estabelecer e manter configurações seguras nos dispositivos de seu ambiente, utilizando *baselines* ou imagens do sistema pré-configuradas, sem se limitar somente a essas medidas.

Art. 26 Onde for suportado, o bloqueio automático de sessões de usuários e ativos deve ser implementado.

Art. 27 O IFSertãoPE deve implementar e gerenciar sistemas de *firewall* nos servidores e *hosts* internos.

Art. 28 O IFSertãoPE deve configurar seus *firewalls* permitindo apenas o tráfego essencial para o funcionamento das operações institucionais.

Art. 29 O gerenciamento dos ativos e *softwares* do IFSertãoPE devem ser realizados através de protocolos seguros como, por exemplo, SSH (*Secure Shell*), HTTPS (*Hypertext Transfer Protocol Secure*) e outras soluções similares.

Art. 30 Os usuários com acesso a contas do tipo *root*, administrador ou equivalentes devem ser devidamente identificados.

Art. 31 Servidores DNS confiáveis (controlados pelo IFSertãoPE ou acessíveis externamente) devem ser configurados e implementados.

Seção V Gestão de Acessos

Art. 32 O IFSertãoPE deverá estabelecer e manter um inventário de todas as contas gerenciadas, devendo incluir contas de usuários e administradores com informações

como nome completo, nome de usuário, departamento e demais que facilitem a rastreabilidade.

Art. 33 O IFSertãoPE deverá criar, definir e manter um processo de concessão e revogação de acessos.

Art. 34 As contas inativas no ambiente do IFSertãoPE devem ser identificadas e desabilitadas.

Art. 35 Diretrizes relacionadas ao uso de senhas serão contempladas no documento.

Art. 36 Onde houver suporte, a Autenticação Multifator deve ser utilizada para:

- I. aplicações expostas externamente;
- II. acesso remoto à rede; e
- III. acesso administrativo.

Art. 37 O compartilhamento de *login*, senha e *tokens* de acesso dentro do ambiente do IFSertãoPE é estritamente proibido.

Art. 38 O usuário é responsável pelas atividades geradas pelas suas credenciais e irá responder por qualquer ação realizada através de seu acesso.

Art. 39 Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Seção VI

Gestão de Vulnerabilidades

Art. 40 O IFSertãoPE deverá definir e manter um processo de gestão de vulnerabilidades para seus ativos.

Art. 41 O IFSertãoPE deverá definir e manter um processo de remediação de vulnerabilidades de acordo com seus riscos.

Art. 42 O IFSertãoPE deve realizar a gestão de *patches*, automatizada quando possível, dos sistemas operacionais e aplicações.

Art. 43 O planejamento de atualizações deve considerar o impacto das mudanças, garantindo que *patches* pequenos de segurança e correções de *bugs* sejam aplicados rapidamente, enquanto atualizações maiores, que incluem novas funcionalidades, tenham um prazo adequado para implementação.

Seção VII

Gestão de Registros

Art. 44 O IFSertãoPE deve definir e manter um processo de gestão de *logs* para fins de auditoria, considerando questões como coleta, revisão e retenção de logs.

Parágrafo único. Os *logs* de auditoria devem ser armazenados de forma segura, garantindo sua integridade.

Art. 45 A sincronização de tempo dos sistemas e dispositivos devem ser padronizados.

Seção VIII

Proteções de Correio Eletrônico e Web

Art. 46 O uso de navegadores e mensageiros eletrônicos atualizados e com suporte ativo deve ser adotado em todo o ambiente institucional do IFSertãoPE.

Art. 47 A implementação de serviços de filtragem para restringir o acesso a sites potencialmente mal-intencionados ou não essenciais às funções internas deve abranger todos os ativos compatíveis.

Art. 48 As demais regras, diretrizes e definições sobre o uso seguro de correio eletrônico, navegação web e ferramentas de comunicação corporativa serão estabelecidas em norma complementar específica.

Seção IX

Defesas Contra *Malware*

Art. 49 Soluções *anti-malware* devem ser utilizadas, onde houver suporte, em todo o ambiente do IFSertãoPE.

Art. 50 A execução e a reprodução automática (*autorun/autoplay*) de mídias removíveis devem ser desabilitadas em todos os ativos do IFSertãoPE.

Seção X

Backups

Art. 51 Diretrizes relacionadas a controles de Backups estão contempladas na Política de Backup e Restauração de Dados.

Seção XI

Gestão de Rede

Art. 52 A infraestrutura de rede deverá ser atualizada periodicamente, garantindo o uso de versões estáveis em seus componentes.

Seção XII

Treinamento e Conscientização

Art. 53 O IFSertãoPE deverá definir e executar um programa de conscientização e treinamentos em segurança da informação, promovendo conhecimentos sobre engenharia social, práticas de autenticação, práticas de tratamento de dados e outros aspectos relevantes.

Art. 54 O conteúdo do programa de conscientização e treinamentos deve ser periodicamente revisado, adequando-se às necessidades atuais.

Seção XIII

Segurança de Aplicações

Art. 55 O desenvolvimento de aplicações no ambiente do IFSertãoPE deve ser realizado considerando as melhores práticas de segurança, garantindo a proteção de dados, a mitigação de vulnerabilidades e a conformidade com normas e regulamentos aplicáveis.

Art. 56 As aplicações desenvolvidas em ambiente interno do IFSertãoPE devem ser testadas em ambiente de homologação antes de serem disponibilizadas em produção.

Seção XIV

Resposta à Incidentes

Art. 57 O IFSertãoPE deverá manter uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Art. 58 Um plano de resposta a incidentes deve estar formalizado e conter: definição de tipos de incidentes, canais de comunicação, responsáveis, fluxos de ação e medidas corretivas.

Art. 59 Todos os incidentes devem ser registrados, categorizados e avaliados quanto à sua gravidade e impacto.

Art. 60 Após cada incidente, deve ser realizada uma análise de causa raiz e atualizar o plano conforme lições aprendidas, caso necessário.

Seção XV

Relacionamento com Terceiros

Art. 61 A relação com terceirizados deve incluir cláusulas contratuais que garantam a proteção das informações institucionais.

§ 1º Nos editais de licitação, nos contratos, convênios, acordos e instrumentos similares de cooperação técnica com entidades prestadoras de serviços para o IFSertãoPE, deverá constar cláusula específica sobre a obrigatoriedade de observância a esta Política, bem como deverá ser exigida, do terceiro contratado, a assinatura do Termo de Responsabilidade.

§ 2º No contrato, acordo, convênio ou instrumento congêneres deverá estar prevista a obrigação da outra parte de divulgar esta Política, bem como suas normas e procedimentos complementares aos seus empregados e prepostos envolvidos em atividades no IFSertãoPE.

CAPÍTULO VII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I

Da Diretoria de Gestão de Tecnologia da Informação

Art. 62 Compete à Diretoria de Gestão de Tecnologia da Informação:

1. Propor, de forma compartilhada, as políticas e diretrizes da área de tecnologia da informação e comunicação, incluindo as de investimento, de acordo com o Plano de Desenvolvimento Institucional e com o Plano Diretor de Tecnologia da Informação.
2. Identificar novas necessidades da Instituição quanto à Tecnologia da Informação e Comunicação e planejar o desenvolvimento de projetos para o atendimento dessas necessidades em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação.
3. Propor, implementar e manter políticas de Segurança da Informação.
4. Propor e supervisionar a execução da política de informatização.
5. Normatizar as metodologias de Tecnologia da Informação e Comunicação.
6. Prestar apoio e assessoria aos campi em assuntos relacionados à Tecnologia da Informação e Comunicação.
7. Prover a infraestrutura de TIC para os serviços de rede corporativos e sistemas de informação.
8. Avaliar os riscos nos projetos de Tecnologia da Informação e Comunicação.
9. Gerenciar os recursos de informática e zelar pela garantia da manutenção e do bom funcionamento dos equipamentos e sistemas de informática no âmbito da Reitoria.
10. Estabelecer padrões, coordenar projetos e oferecer soluções para ambientes informatizados.
11. Receber e administrar as prioridades de desenvolvimento de novos sistemas.
12. Representar a instituição nos foros específicos da área.

13. Gerir contratos com fornecedores de bens e serviços de Tecnologia da Informação e Comunicação.

14. Executar outras funções que, por sua natureza, lhe estejam afetas ou lhe tenham sido atribuídas.

Seção II

Do Comitê de Governança Digital

Art. 63 Compete ao Comitê de Governança Digital:

1. Definir prioridades para os projetos e ações de TIC.
2. Auxiliar na tomada de decisão em relação aos recursos orçamentários para a viabilização da implementação dos planos.
3. Deliberar sobre as estratégias, planos e políticas de TIC para o IFSertãoPE.

Seção III

Do Comitê Gestor de Segurança da Informação

Art. 64 Compete ao Comitê Gestor de Segurança da Informação:

1. assessorar a implementação das ações de segurança da informação;
2. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
3. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;
4. propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;
5. deliberar sobre normas internas de segurança da informação.
6. monitorar a execução do Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) e Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), sob a perspectiva da segurança da informação para sugerir e recomendar alterações que se façam necessárias.

7. promover a cultura de segurança da informação no IFSertãoPE, com a realização de campanhas de conscientização dos usuários quanto à política de segurança da informação.
8. proposição, acompanhamento e divulgação dos planos de ações para aplicação da PSI.
9. Propor programa orçamentário específico para as ações de segurança da informação.

Seção IV

Do Gestor de Segurança da Informação

Art. 65 Compete ao Gestor de Segurança da Informação:

- I. coordenar o Comitê Gestor de Segurança da Informação;
- II. coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;
- III. assessorar a Comitê de Governança Digital na implementação da Política de Segurança da Informação;
- IV. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- V. promover a divulgação da política e das normas internas de segurança da informação do IFSertãoPE a todos os servidores, usuários e prestadores de serviços que trabalham na Instituição;
- VI. incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;
- VII. propor recursos necessários às ações de segurança da informação;
- VIII. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

IX. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI. manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Seção V

Do Gestor de Tecnologia da Informação

Art. 66 Compete ao Gestor de Tecnologia da Informação, dentre outras atribuições dispostas na legislação vigente, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação, considerando a cadeia de suprimentos relacionada à solução.

Seção VI

Do Encarregado pelo Tratamento dos Dados Pessoais

Art. 67. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e nos normativos emitidos pela Agência Nacional de Proteção de Dados (ANPD):

I - conduzir o diagnóstico e a gestão da privacidade no âmbito institucional;

II - orientar os gestores e proprietários dos ativos de informação quanto ao planejamento, implementação e melhoria contínua dos controles de privacidade em operações que envolvam dados pessoais ou dados pessoais sensíveis;

III - atuar como canal de comunicação entre o IFSertãoPE, os titulares dos dados e a ANPD.

Parágrafo único. O Encarregado pelo Tratamento dos Dados Pessoais manterá canal de comunicação público e acessível, por meio eletrônico e físico, para o atendimento e o exercício dos direitos dos titulares de dados pessoais, nos termos da legislação vigente e do Programa de Privacidade e Segurança da Informação do IFSertãoPE.

Seção VII

Do Responsável pela Unidade de Controle Interno

Art. 68 Compete à Auditoria Interna, no exercício de suas atribuições institucionais, avaliar, de forma independente e objetiva, a adequação e a eficácia dos processos de governança, gerenciamento de riscos e controles internos relacionados à segurança da informação, observadas as normas aplicáveis à atividade de auditoria interna governamental.

Seção VIII

Da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos

Art. 69 Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

- I** - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no IFSertãoPE;
- II** - monitorar as redes computacionais, os sistemas e o uso dos ativos de informação institucionais sob a ótica da segurança cibernética;
- III** - detectar e analisar ataques, intrusões e anomalias de segurança;
- IV** - tratar e mitigar os incidentes de segurança da informação no âmbito institucional;
- V** - identificar vulnerabilidades, ameaças e artefatos maliciosos;
- VI** - auxiliar no restabelecimento e na recuperação dos sistemas de informação afetados;

VII - promover a cooperação com outras equipes, participando de fóruns, comunidades e redes de segurança da informação;

VIII - manter ponto focal de contato com o Centro de Atendimento a Incidentes de Segurança da RNP (CAIS/RNP);

IX - reportar incidentes cibernéticos relevantes ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR-Gov); e

X - observar as diretrizes e o regimento interno da ETIR-IFSertãoPE estabelecidos em norma complementar específica.

Seção IX Dos Usuários

Art. 70 Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e demais normas específicas de segurança da informação do IFSertãoPE.

Art. 71 Os usuários deverão comunicar imediatamente à ETIR qualquer suspeita de incidente de segurança. Qualquer comunicado de incidentes de segurança deve ser direcionado para o e-mail: .

CAPÍTULO VIII

DAS PENALIDADES

Art. 72. O descumprimento das diretrizes desta Política e de suas normas complementares constituirá infração passível de apuração e de aplicação de medidas administrativas, suspensão preventiva de acessos e sanções disciplinares ou contratuais, observado o devido processo legal, o contraditório e a ampla defesa.

§ 1º As infrações serão avaliadas e classificadas em leves, moderadas e graves, considerando o parecer técnico de impacto na confidencialidade, integridade, disponibilidade e legalidade emitido pelo Comitê Gestor de Segurança da Informação (CGSI) ou pela ETIR-IFSertãoPE.

§ 2º A instrução, o enquadramento final e a aplicação das sanções caberão:

I - à Corregedoria ou comissão disciplinar competente, mediante Processo Administrativo Disciplinar (PAD) ou sindicância, no caso de servidores efetivos ou temporários;

II - à fiscalização e gestão do contrato, no caso de empregados de empresas contratadas, prestadores de serviço e terceirizados, observadas as cláusulas contratuais e a legislação de licitações;

III - às instâncias acadêmicas ou administrativas próprias, conforme regimento disciplinar do IFSertãoPE, no caso de discentes e colaboradores externos.

§ 3º A reincidência em infrações, bem como a ocorrência de descumprimentos classificados como moderados ou graves, poderá implicar a suspensão cautelar preventiva ou a revogação das credenciais e perfis de acesso do usuário, mediante justificativa fundamentada da área de Segurança da Informação.

Parágrafo único. Para as infrações classificadas como graves pelo Comitê Gestor de Segurança da Informação (CGSI) ou Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), poderá ocorrer o bloqueio temporário de contas e perfis com o objetivo de sanar o problema, encaminhando a continuidade do bloqueio para instâncias superiores.

CAPÍTULO IX

DA ATUALIZAÇÃO

Art. 73 Esta Política de Segurança da Informação deve ser revisada quando necessário ou respeitando o **prazo máximo de vigência de 04 anos**, podendo ter revisão anualmente.

Art. 74 A periodicidade para atualização e revisão das ações previstas nas diretrizes desta política deverá ser definida por meio de normativo interno, especificando os casos individualmente.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 75 A implementação das diretrizes dispostas nesta política dependerá da disponibilidade de recursos financeiros, humanos e tecnológicos do IFSertãoPE.

Art. 76 Os sistemas legados incapazes de implementar as ações previstas neste normativo deverão ser identificados, por meio do inventário de ativos, juntamente aos seus riscos e justificativas, a fim de que sejam adotadas medidas para mitigar tais riscos.

Art. 77 Os editais de licitação, contratos, convênios, acordos e demais instrumentos de cooperação técnica com entidades prestadoras de serviços para o IFSertãoPE devem conter uma cláusula específica sobre a obrigatoriedade de cumprimento desta Política, além da exigência de assinatura do Termo de Responsabilidade pela entidade contratada.

Art. 78 Esta Política entra em vigor na data de sua publicação.

ANEXO I

REFERÊNCIA LEGAL E BOAS PRÁTICAS

Orientação	Secção
Diretrizes Federais	
Decreto Nº 12.198/2024 - Estratégia Federal de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados	Em sua íntegra
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I
Decreto Nº 12.572/2025 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2 CAPÍTULO II - Art.3 CAPÍTULO VI - Art.10
Decreto Nº 12.573/2025 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Portaria nº 93/GSI/PR, de 18 de outubro de 2021 - Aprova o glossário de segurança da informação.	Em sua íntegra
Instrução Normativa nº 01/GSI/PR, de 27 de maio de 2020 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.	Art.12, Inciso IV, alínea c
Acórdão nº 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
Frameworks	
ABNT NBR ISO/IEC 27002: 2022. Código de Prática para controles de Segurança da Informação	Em sua íntegra
NIST SP 800-53 Rev. 5	Em sua íntegra
Center for Internet Security (2021) - CIS Controls Version 8	Em sua íntegra
Programa de Privacidade e Segurança da Informação da Secretaria de Governo Digital	
Guia do Framework de Privacidade e Segurança da Informação	Em sua íntegra
Modelo de Política de Segurança da Informação – PPSI	Em sua íntegra
INSTRUÇÃO NORMATIVA SGD/MGI Nº 4, DE 14 DE JANEIRO DE 2026	Em sua íntegra

Privacidade e Proteção de Dados	
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	Capítulo VII - Seção I – Art. 46, Seção II, art. 50
Guia Orientativo - Tratamento de dados pessoais pelo Poder Público	Em sua íntegra