Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
Diretoria de Gestão Estratégica

Política de Segurança da Informação do Cefet/RJ

Institui a Política de Segurança da Informação e das Comunicações, aplicável a todas as unidades do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca. Esta política deverá ser adotada e cumprida por todos os servidores, colaboradores, consultores externos, estagiários, alunos e prestadores de serviço que exerçam atividades ou tenham acesso a dados ou informações no ambiente do Cefet/RJ.

CAPÍTULO I

DO OBJETIVO

Art. 1º A Política de Segurança da Informação (POSIN) do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) tem como objetivo estabelecer os princípios, diretrizes, responsabilidades e práticas para a proteção das informações do Centro, garantindo sua confidencialidade, integridade e disponibilidade. A POSIN visa assegurar o uso adequado das informações, mitigar riscos à segurança da informação e assegurar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normas vigentes.

Parágrafo único. Os princípios, objetivos, diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta POSIN devem estar alinhados ao Plano de Desenvolvimento Institucional (PDI) e ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), mantendo consonância com os valores institucionais do Cefet/RJ.

CAPÍTULO II

DO ESCOPO

Art. 2º A POSIN aplica-se a todos os ativos de informação do Cefet/RJ, incluindo dados, sistemas, aplicativos, dispositivos e redes.

Art. 3º A POSIN vigora em todas as instalações físicas administradas ou utilizadas pelo Cefet/RJ, e refere-se aos aspectos estratégicos, estruturais e organizacionais, estabelecendo a base para a elaboração dos demais documentos normativos que integrarão sua área de atuação.

Art. 4º As diretrizes, normas complementares e manuais de procedimentos da POSIN do Cefet/RJ aplicam-se a toda a comunidade institucional, em seus diversos níveis hierárquicos e vínculos - incluindo colaboradores, funcionários, contratados, parceiros e terceiros que oficialmente executem atividades vinculadas à atuação do Cefet/RJ - e que, em qualquer momento, necessitem utilizar os recursos de tecnologia da informação e comunicação (TIC).

Art. 5º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Cefet/RJ deverão estar em conformidade com esta POSIN.

CAPÍTULO III

DOS TERMOS E DEFINIÇÕES

Art. 6º Os termos-chave, siglas e conceitos utilizados nesta política têm como referência as definições apresentadas no art. 5° da LGPD, além da Portaria GSI/PR n° 93, de 18 de outubro de 2021 - Glossário de Segurança da Informação, instituído pelo Gabinete de Segurança Institucional da Presidência da República[1] e suas atualizações.

Art. 7º A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

CAPÍTULO IV

DOS PRINCÍPIOS E DIRETRIZES

Art. 8º As ações de segurança da informação do Cefet/RJ são norteadas pelos princípios constitucionais e administrativos que regem 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 Cefet/RJ;

III — Economicidade na proteção dos ativos de informação;IV - Respeito ao acesso à informação, à proteção de dados pessoais e à preservação da privacidade;

IV — Observância da publicidade como preceito geral e do sigilo como exceção;

V — Responsabilização do usuário pelos atos que comprometam a segurança dos ativos de informação;

[1] https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370

VI — Alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do Cefet/RJ e com as demais normas específicas de segurança da informação da Administração Pública Federal;

VII — Conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis; e

VIII — Educação e comunicação como alicerces fundamentais para o fomento da cultura de segurança da informação.

Art. 9º Estas diretrizes constituem os principais pilares da gestão de segurança da informação, norteando a elaboração de políticas, planos e normas complementares no âmbito desta instituição, e visam garantir os princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 10 As normas, procedimentos, manuais e metodologias de segurança da informação do Cefet/RJ devem considerar, como referência, além dos normativos vigentes, as melhores práticas reconhecidas em segurança da informação.

Art. 11 As ações de segurança da informação devem:

I — considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do Cefet/RJ;

II — ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do Cefet/RJ;

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. 12 A administração e gestão da segurança da informação em ambiente computacional do Cefet/RJ ficarão sob responsabilidade do Departamento de Tecnologia da Informação (DTINF), subordinado à Diretoria de Gestão Estratégica do Cefet/RJ.

Art. 13 O DTINF será o responsável pelas normas e procedimentos institucionais necessários para garantir a segurança e mitigar riscos ao ambiente de Tecnologia da Informação e Comunicação – TIC do Cefet/RJ.

Parágrafo único. As normas e procedimentos institucionais citados no caput deverão ser homologados pela Diretoria de Gestão Estratégica.

Art. 14 Todos os servidores e demais colaboradores que atuem no gerenciamento de sistemas, acesso à informação e atividades relacionadas à segurança da informação são corresponsáveis pela execução dos planos, políticas e procedimentos de segurança da informação, bem como pela mitigação de incidentes de segurança da informação e pela notificação e resolução célere destes.

Art. 15 Os servidores deverão ser capacitados para o desenvolvimento de competências em privacidade e segurança da informação, com a devida comunicação aos níveis estratégico, tático e operacional do Cefet/RJ.

Art. 16 A segurança da informação é responsabilidade de qualquer usuário, não apenas da área de TIC; desta forma, deverá refletir-se em hábitos, atitudes, responsabilidades e cuidados constantes no momento do uso, solicitação de aprovação de recursos e demais atividades correlatas.

Art. 17 Compete à Direção-Geral, às diretorias, aos Campi, Comitês e Comissões delegadas monitorar o desempenho e avaliar a concepção, a implementação e os resultados da política de segurança da informação e das normas internas de segurança da informação.

CAPÍTULO V

DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 18 A estrutura de Gestão de Segurança da Informação é composta por:

I — Direção-geral;

II — Diretorias Sistêmicas;

III — Diretorias dos Campi em seu respectivo escopo;

IV — Comitê de Segurança da Informação;

V — Gestor de Segurança da Informação;

VI — Gestor do Departamento de Tecnologia da Informação;

VII — Encarregado pelo Tratamento de Dados Pessoais;

VIII — Responsável pela Unidade de Controle Interno;

IX — Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos;

X — Setores de informática - SINFOs dos Campi; e

XI — Usuários de Informação.

Art. 19 Compete à Direção-Geral do Cefet/RJ:

I — fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do Cefet/RJ, bem como tratar as ações e decisões de segurança da informação com nível adequado de relevância e prioridade; e

II — formalizar e aprovar a Política de Segurança da Informação do Cefet/RJ, bem como suas alterações e atualizações.

Art. 20 Caberão às Diretorias Sistêmicas e às Diretorias de Campi:

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

II — incorporar aos processos de trabalho de sua unidade ou área práticas inerentes à TICs;

III — adotar as medidas administrativas necessárias para aplicação de ações corretivas nos casos de comprometimento da SI por parte dos usuários sob sua supervisão;

IV — informar ao Departamento de Gestão de Pessoas do Cefet/RJ a movimentação de pessoal de sua unidade para que ocorra a garantia dos mecanismos de autenticação e autorização; e

V — manter lista atualizada dos ativos de informação sob sua responsabilidade, com seus respectivos gestores.

Art. 21 Compete ao Comitê de Segurança da Informação:

I — assessorar na implementação das ações de segurança da informação;

II — constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III — propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

IV — deliberar sobre normas internas de segurança da informação; e

V — deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e encaminhar à Direção-Geral para aprovação do processo contendo os documentos sobre a avaliação de conformidade.

Parágrafo único. A composição, estrutura, recursos e funcionamento do Comitê de Segurança da Informação serão definidos em portaria emitida pelo Cefet/RJ, de acordo com a legislação vigente.

Art. 22 Compete ao Gestor de Segurança da Informação:

I — 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;

II — assessorar a Direção-Geral na implementação desta POSIN;

III — estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV — promover a divulgação da política e das normas internas de segurança da informação a todos os servidores, usuários e prestadores de serviços do Cefet/RJ;

V — incentivar estudos de novas tecnologias e seus eventuais impactos relacionados à segurança da informação;

VI — propor recursos necessários às ações de segurança da informação;

VII — acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

VIII — verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

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

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

Parágrafo único. O Gestor de Segurança da Informação do Cefet/RJ será designado em Portaria, de acordo com a legislação vigente.

Art. 23 Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Art. 24 Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Art. 25 Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 26 Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos:

I — facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no Cefet/RJ;

II — monitorar as redes computacionais;

III — detectar e analisar ataques e intrusões;

IV — tratar incidentes de segurança da informação;

V — identificar vulnerabilidades e artefatos maliciosos;

VI — recuperar sistemas de informação;

VII — promover a cooperação com outras equipes e participar de fóruns e redes relativos à segurança da informação.

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos serão definidos em Portaria emitida pelo Cefet/RJ, de acordo com a legislação vigente.

Art. 27 Caberá aos Setores de Informática dos Campi:

I — desempenhar atividades afetas à área de Tecnologia da Informação e Comunicação aquelas executadas em conformidade com as recomendações emanadas pelo Departamento de Tecnologia da Informação (DTINF), pelo Comitê de Governança, Desenvolvimento Digital, Riscos e Controles (CGDDRC) e pelo Comitê de Segurança da Informação (CSI)

Art. 28 Caberá aos usuários de informação:

I — conhecer, cumprir e fazer cumprir esta Política e as demais normas específicas de segurança da informação do Cefet/RJ;

II — comunicar formalmente, via sistema de chamados ou e-mail, os incidentes que afetam a segurança dos ativos de informação ao DTINF; e

III — participar de treinamentos e orientações periódicas sobre o tema, utilizando diversos meios para consolidar e contribuir para a melhoria contínua tanto da Política de Segurança da Informação (POSIN) quanto da Segurança da Informação (SI) no âmbito do CEFET.

Art. 29 Caberá aos terceiros e fornecedores, conforme previsto em contrato:

I — tomar conhecimento desta POSIN;

II — observar, no exercício de suas atividades, a íntegra desta POSIN;

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

IV — fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

Art. 30 A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I — tratamento da informação;

II — segurança física e do ambiente;

III — gestão de incidentes em segurança da informação;

IV — gestão de ativos;

V — gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI — controles de acesso;

VII — gestão de riscos;

VIII — gestão de continuidade; e

IX — auditoria e conformidade.

§ 1° O Comitê de Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

§ 2° Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

Art. 31 As políticas, normas, procedimentos, orientações ou manuais de que trata o §2° do Art. 30 devem abordar, no mínimo, aspectos relacionados:

I — à conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

II — à classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III — à proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

IV — ao uso aceitável da informação e à utilização de mídias de armazenamento;

V — à entrada e saída de ativos de informação das instalações da organização;

VI — aos perímetros de segurança da instituição;

VII — aos controles de acesso baseados no princípio do menor privilégio;

VIII — às etapas de identificação, contenção, erradicação e recuperação e atividades pós-incidente;

IX — aos critérios para a comunicação de incidentes aos titulares de dados pessoais e à ANPD;

X — ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;

XI — à Política de Gestão de Ativos da organização, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para a organização; a manutenção de inventário atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

XII — à utilização adequada dos recursos operacionais e de comunicações fornecidos pelo Cefet/RJ, a serem utilizados para fins profissionais, relacionados às atividades da instituição, em conformidade com seus princípios éticos e profissionais, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação do órgão;

XIII — aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV — ao acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XV — ao uso de mídias sociais, à divulgação de informações nas mídias sociais, ao uso de contas pessoais para fins profissionais e à interação com estranhos nas mídias sociais;

XVI — às políticas e procedimentos para o uso da computação em nuvem, à seleção de provedores de serviços em nuvem, à segurança dos dados na nuvem e à conformidade com as leis e regulamentos aplicáveis;

XVII — às políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação do Cefet/RJ;

XVIII — às políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente da instituição, dos seus ativos de informação e das ameaças à segurança da informação; a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência; a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento; o tratamento dos riscos

identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos;

XIX — às políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que o órgão possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XX — às políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças; e

XXI — às políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

CAPÍTULO VI

DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

Art. 32 É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo Cefet/RJ para acesso, guarda e divulgação de material incompatível com o ambiente e objetivos do serviço do Centro, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 33 São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela instituição.

Art. 34 É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 35 É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 36 As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através do e-mail segur@cefet-rj.br.

Art. 37 O cumprimento desta Política, bem como dos normativos que a complementam, deve ser avaliado pelo Cefet/RJ periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 38 A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme

a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 39 Esta Política, bem como o conjunto de instrumentos normativos gerados a partir dela, deverá ser revisado anualmente ou por deliberação do Comitê de Segurança da Informação.

Art. 40 Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos complementares serão decididos pelo Diretor de Gestão Estratégica, ouvido o Comitê Gestor de Segurança da Informação - CSI do Cefet/RJ.

Art. 41 A presente política entrará em vigor a partir da data de sua publicação.