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, 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.

Seção 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 por objetivo estabelecer princípios, diretrizes, responsabilidades e práticas para a proteção da informação e para o uso seguro dos ativos, recursos e ambientes de tecnologia da informação e comunicação que a suportam, de modo a garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações.

Parágrafo único. A POSIN visa assegurar o uso adequado das informações e dos recursos tecnológicos a elas associados, mitigar riscos à segurança da informação e promover o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e das demais normas vigentes.

Seção II

Do Escopo

Art. 2º A POSIN aplica-se aos ativos de informação do Cefet/RJ e aos ativos, recursos, serviços e ambientes de tecnologia da informação e comunicação utilizados para criar, processar, armazenar, transmitir, custodiar, proteger ou disponibilizar informações no âmbito institucional.

Art. 3º A POSIN aplica-se em todas as instalações físicas e ambientes tecnológicos administrados ou utilizados pelo Cefet/RJ e abrange os aspectos estratégicos, estruturais, organizacionais e operacionais necessários à segurança da informação, servindo de base

para a elaboração dos demais documentos normativos integrantes de seu campo 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, servidores, contratados, parceiros e terceiros que oficialmente executem atividades vinculadas à atuação do Cefet/RJ e que, em qualquer momento, necessitem utilizar ativos, recursos ou serviços de tecnologia da informação e comunicação.

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

Seção III

Dos Termos e Definições

Art. 6º Para os fins desta Política, consideram-se:

I — Ativo de informação: dado, informação ou conjunto informacional de interesse institucional, independentemente do meio em que esteja armazenado, processado, transmitido ou disponibilizado.

II — Ativo de tecnologia da informação e comunicação: equipamentos, dispositivos, sistemas, aplicações, serviços, redes, infraestruturas, ambientes computacionais e demais recursos tecnológicos utilizados para suportar o tratamento, o armazenamento, a transmissão, a proteção ou a disponibilização de informações.

III — Usuário de informação: pessoa física que, em razão de vínculo funcional, acadêmico, contratual, eventual ou autorizado, utilize, acesse, manuseie ou administre ativos de informação do Cefet/RJ.

IV — Proprietário do ativo de informação: unidade ou autoridade responsável pela definição da finalidade, classificação, nível de criticidade, regras de acesso e requisitos de proteção de determinado ativo de informação.

V — Custodiante do ativo de informação: unidade ou agente responsável pela guarda, operação, manutenção ou suporte técnico do ativo de informação, em conformidade com as diretrizes estabelecidas pelo seu proprietário.

VI — Incidente de segurança da informação: evento confirmado ou sob suspeita que comprometa ou possa comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade da informação ou dos ativos que a suportam.

VII — Incidente físico de segurança da informação: incidente de segurança da informação relacionado a ambientes, instalações, documentos, mídias, equipamentos ou outros elementos materiais, sem prejuízo de seus reflexos sobre informações em meio digital.

VIII — Incidente cibernético: incidente de segurança da informação que envolva sistemas, redes, serviços digitais, dispositivos computacionais, ambientes tecnológicos ou ativos de tecnologia da informação e comunicação.

IX — Vulnerabilidade: fragilidade, deficiência ou condição de ativo, processo ou controle que possa ser explorada, intencionalmente ou não, para comprometer a segurança da informação.

X — Homologação: procedimento formal pelo qual a instituição verifica e declara que determinado recurso de tecnologia da informação e comunicação atende aos requisitos técnicos, de segurança, interoperabilidade, licenciamento e suporte definidos para seu uso institucional.

XI — Autorização excepcional: permissão formal, motivada, temporária e registrada, concedida pela autoridade competente para uso de recurso, solução ou procedimento não homologado, mediante justificativa, análise de riscos e definição de responsabilidades e salvaguardas.

XII — Terceiro: pessoa física ou jurídica sem vínculo estatutário ou empregatício direto com o Cefet/RJ que, por contrato, convênio, parceria, cooperação, pesquisa, extensão, prestação de serviço ou outra relação jurídica, tenha acesso a ativos de informação institucionais.

XIII — Fornecedor: terceiro responsável pelo fornecimento de bens ou serviços, inclusive serviços continuados, serviços em nuvem, software, suporte técnico, desenvolvimento, manutenção ou operação de soluções de tecnologia da informação e comunicação.

XIV — Canal institucional de comunicação de incidente: meio formal definido pelo Cefet/RJ para registro, escalonamento, tratamento e acompanhamento de incidentes, vulnerabilidades ou violações relacionadas à segurança da informação.

XV — Uso aceitável: utilização de ativos de informação e recursos de tecnologia da informação e comunicação em conformidade com a finalidade institucional, a legislação aplicável, os normativos internos e os requisitos de segurança, ética, privacidade e proteção de dados.

XVI — Classificação da informação: processo de atribuição de nível de sensibilidade, restrição de acesso ou criticidade à informação, considerado seu valor, uso, requisitos legais e impactos potenciais de divulgação, alteração, indisponibilidade ou perda.

XVII — Análise de riscos: processo sistemático de identificação, avaliação e tratamento de riscos que possam afetar ativos de informação, considerando ameaças, vulnerabilidades, probabilidade de ocorrência, impacto e controles existentes.

Art. 7º Os termos-chave, siglas e conceitos utilizados nesta Política têm como referência o art. 5º da Lei nº 13.709, de 14 de agosto de 2018, e o Glossário de Segurança da Informação aprovado pelo Gabinete de Segurança Institucional da Presidência da República, bem como suas atualizações.

Parágrafo único. Ato complementar deverá consolidar e atualizar, sempre que necessário, as definições mínimas aplicáveis a esta Política.

Art. 8º A Política de Segurança da Informação e os normativos dela decorrentes integram o arcabouço normativo da Gestão de Segurança da Informação do Cefet/RJ.

Seção IV

Dos Princípios e Diretrizes

Art. 9º 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;

V — observância da publicidade como preceito geral e do sigilo como exceção;

VI — responsabilização do usuário pelos atos que comprometam a segurança dos ativos de informação;

VII — 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;

VIII — conformidade das normas e das ações de segurança da informação com a legislação e os regulamentos aplicáveis; e

IX — educação e comunicação como alicerces fundamentais para o fomento da cultura de segurança da informação.

Art. 10 Estas diretrizes constituem os principais pilares da gestão de segurança da informação, norteando a elaboração de políticas, planos e normas complementares no âmbito do Cefet/RJ, e visam garantir os princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 11 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. 12 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, inclusive quanto aos meios físicos e digitais que a suportam; e

IV — visar à prevenção da ocorrência de incidentes de segurança da informação, físicos ou cibernéticos.

Art. 13 A governança da segurança da informação observará as competências previstas nesta Política.

Parágrafo único. Compete ao Departamento de Tecnologia da Informação (DTINF), no âmbito técnico-operacional, administrar e implementar controles de segurança da informação em ambiente computacional, sem prejuízo das atribuições das demais instâncias de gestão de segurança da informação do Cefet/RJ.

Art. 14 O DTINF será responsável pela elaboração de normas e procedimentos institucionais necessários à garantia da segurança e à mitigação de riscos no ambiente de tecnologia da informação e comunicação do Cefet/RJ.

Parágrafo único. As normas e procedimentos institucionais referidos no caput deverão ser aprovados pelas instâncias competentes, nos termos desta Política.

Art. 15 Todos os servidores e demais colaboradores que atuem no gerenciamento de sistemas, no acesso à informação e em atividades relacionadas à segurança da informação são corresponsáveis pela observância dos planos, políticas e procedimentos de segurança da informação, bem como pela prevenção, identificação, comunicação e tratamento, no âmbito de suas atribuições, de incidentes de segurança da informação, físicos ou cibernéticos.

Parágrafo único. A comunicação e o tratamento de incidentes de segurança da informação, físicos ou cibernéticos, observarão os conceitos, fluxos, níveis de criticidade e canais institucionais definidos nesta Política e em seus normativos complementares.

Art. 16 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. 17 A segurança da informação é responsabilidade de todo usuário, não apenas da área de tecnologia da informação e comunicação, devendo refletir-se em hábitos, atitudes, responsabilidades e cuidados constantes no uso de ativos, recursos e serviços institucionais.

Art. 18 Compete à Direção-Geral, aos diretores sistêmicos, aos diretores de *campi*, ao Comitê de Segurança da Informação (CSI) e ao Comitê de Usuários dos Sistemas de Informação monitorar o desempenho e avaliar a concepção, a implementação e os resultados desta Política e das normas internas de segurança da informação.

§ 1º O Comitê de Usuários dos Sistemas de Informação, apresentado no caput deste artigo, será composto por representantes indicados pelos diretores sistêmicos, sendo dois representantes por cada uma das áreas de ensino, pesquisa e extensão, e um representante por cada uma das áreas de administração e planejamento, e gestão estratégica.

§ 2º O Comitê de Usuários dos Sistemas de Informação deverá atuar de forma articulada com o Comitê de Segurança da Informação e com as áreas técnicas competentes, contribuindo para a avaliação, o aperfeiçoamento e a adequação das normas e práticas de segurança da informação às necessidades institucionais, bem como para a definição de requisitos e necessidades dos usuários do Centro.

§ 3º A composição detalhada, o funcionamento e as competências complementares do Comitê de Usuários dos Sistemas de Informação serão definidos em ato próprio.

Seção V

Da Gestão de Segurança da Informação

Art. 19 A estrutura de Gestão de Segurança da Informação é composta por:

I — Direção-Geral;

II — diretorias sistêmicas;

III — diretorias dos Campi, em seus respectivos escopos;

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 Setorial de Integridade, Transparência e Acesso à Informação, ou unidade equivalente formalmente designada;

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

X — setores de informática dos Campi; e

XI — usuários de informação.

Art. 20 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. 21 Compete às diretorias sistêmicas e às diretorias de Campi:

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

II — incorporar aos processos de trabalho de sua unidade ou área práticas de segurança da informação, privacidade e proteção de dados compatíveis com suas atividades;

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

IV — informar ao setor competente de gestão de pessoas a movimentação de pessoal de sua unidade para viabilizar a gestão dos mecanismos de autenticação e autorização; e

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

Art. 22 Compete ao Comitê de Segurança da Informação:

I — assessorar a 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 a partir dos resultados de avaliações de conformidade e encaminhá-las à Direção-Geral para aprovação.

Parágrafo único. A composição, a estrutura, os recursos e o funcionamento do Comitê de Segurança da Informação serão definidos em ato próprio, de acordo com a legislação vigente.

Art. 23 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 Cefet/RJ, observada 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 interlocução institucional em assuntos relativos à segurança da informação com órgãos e entidades competentes.

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

Art. 24 Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições previstas na legislação vigente, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicação, considerando a cadeia de suprimentos relacionada à solução.

Art. 25 Compete ao Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições previstas na legislação vigente, 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 tratamento de dados pessoais.

Art. 26 Compete ao responsável pela unidade referida no art. 19, VIII, dentre outras atribuições legais, coordenar e monitorar, no âmbito de suas competências, as ações de integridade, transparência e acesso à informação, promovendo articulação com as

funções de ouvidoria, corregedoria, ética, gestão de riscos, controle interno, segurança da informação e proteção de dados.

Art. 27 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 de natureza cibernética;

V — identificar vulnerabilidades e artefatos maliciosos;

VI — recuperar sistemas de informação; e

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

Parágrafo único. A composição, a estrutura, os recursos e o funcionamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos serão definidos em ato próprio, de acordo com a legislação vigente.

Art. 28 Compete aos setores de informática dos Campi executar, em seus respectivos âmbitos, as atividades de tecnologia da informação e comunicação e de segurança da informação em conformidade com as diretrizes, normas, padrões e orientações expedidos pelo DTINF e pelas instâncias de governança formalmente competentes.

Art. 29 Compete 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, pelos canais institucionais definidos, os incidentes que afetem a segurança dos ativos de informação; e

III — participar de treinamentos e orientações periódicas sobre o tema, contribuindo para a melhoria contínua da Política de Segurança da Informação e da segurança da informação no âmbito do Cefet/RJ.

Art. 30 Compete aos terceiros e fornecedores, conforme previsto em contrato:

I — tomar conhecimento desta POSIN;

II — observar, no exercício de suas atividades, o inteiro teor 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 a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

Art. 31 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 de segurança da informação;

IV — gestão de ativos;

V — gestão do uso dos recursos operacionais e de comunicações, tais como correio eletrônico, 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.

§ 1º 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.

§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deverá 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 com as boas práticas de segurança da informação.

Art. 32 As políticas, normas, procedimentos, orientações ou manuais de que trata o § 2º do art. 31 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 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 instituição;

VI — aos perímetros de segurança da instituição;

VII — às diretrizes, normas e procedimentos de segurança física e do ambiente, abrangendo controle de acesso a áreas e instalações, guarda e proteção de documentos, mídias e equipamentos, descarte seguro, gestão de visitantes e prestadores de serviço, prevenção de acessos físicos não autorizados e proteção de ambientes críticos ou sensíveis;

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

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

X — aos critérios, fluxos, responsabilidades e prazos para a comunicação de incidentes de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados e aos titulares, observado o disposto no art. 48 da Lei nº 13.709, de 14 de agosto de 2018, e na regulamentação da ANPD;

XI — ao Plano de Gestão de Incidentes de Segurança da Informação, de forma a considerar diferentes cenários;

XII — à política de gestão de ativos da organização, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade para a organização, a manutenção de inventário atualizado, o uso aceitável, o mapeamento de vulnerabilidades, ameaças e interdependências, o monitoramento de ativos e a investigação de sua operação e uso quando houver indícios de quebra de segurança e ou privacidade;

XIII — à utilização adequada dos recursos operacionais e de comunicações fornecidos pelo Cefet/RJ, a serem utilizados para fins institucionais, em conformidade com seus princípios éticos e profissionais;

XIV — aos procedimentos para o uso de correio eletrônico, o envio de informações confidenciais, a instalação de software de proteção e a abertura de anexos e links;

XV — ao acesso à internet, ao download de arquivos, aos controles de navegação e à instalação de software não autorizado;

XVI — ao uso de mídias sociais, à divulgação de informações, ao uso de contas pessoais para fins profissionais e às cautelas de segurança na interação em ambientes digitais;

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

XVIII — às políticas e procedimentos para o controle de acesso, inclusive uso de autenticação multifator, segregação de funções, trilhas de auditoria, rastreamento e gestão de desligamento ou afastamento de colaboradores e parceiros;

XIX — às políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar os ativos institucionais, abrangendo identificação, análise, avaliação, tratamento, aceitação e documentação dos riscos;

XX — às políticas e procedimentos para gestão de continuidade de negócios, incluindo plano de continuidade e realização de testes e exercícios periódicos; e

XXI — às políticas e procedimentos para auditoria e conformidade, abrangendo plano de verificação de conformidade e relatório de avaliação de conformidade.

Seção VI

Das Vedações e Disposições Finais

Art. 33 É vedada a utilização de ativos de tecnologia da informação e comunicação que:

I — infrinjam a legislação vigente;

II — violem direitos autorais;

III — sejam incompatíveis com o ambiente institucional, considerado em seus aspectos físicos, lógicos e operacionais;

IV — sejam incompatíveis com a natureza e os objetivos de uma instituição pública de educação superior; ou

V — constituam risco ou impliquem dano material, moral ou à imagem de qualquer pessoa ou da instituição.

Art. 34 São vedados a instalação e o uso de ativos de tecnologia da informação e comunicação em desconformidade com as normas, os padrões e as orientações estabelecidos pelas instâncias competentes referidas no art. 18.

Art. 35 É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta, senha ou certificação digital, de uso pessoal e intransferível, fornecidos aos usuários.

Art. 36 É vedada a exploração de vulnerabilidades em ativos do Cefet/RJ, ressalvadas as atividades de teste, auditoria, pesquisa ou resposta a incidentes previamente autorizadas pela autoridade competente.

Parágrafo único. As vulnerabilidades identificadas deverão ser comunicadas imediatamente ao DTINF, à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos ou ao canal institucional definido em norma específica.

Art. 37 As comunicações de incidentes, vulnerabilidades e violações desta Política deverão ser realizadas pelos canais institucionais formalmente definidos, inclusive o canal técnico para incidentes de segurança da informação e o canal de integridade ou de ouvidoria, quando cabível, sem prejuízo do uso do endereço eletrônico institucional destinado à segurança da informação, definido por ato do chefe do departamento de tecnologia da informação.

Art. 38 O cumprimento desta Política, bem como dos normativos que a complementam, deverá ser avaliado periodicamente por meio de verificações de conformidade, com vistas a aferir o grau de aderência aos requisitos de segurança da informação e às cláusulas de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 39 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 civil e penal, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 40 Esta Política e os instrumentos normativos dela decorrentes deverão ser revisados periodicamente, em prazo não superior a quatro anos, sem prejuízo de revisão anterior quando necessária por alteração legal, normativa, estrutural, tecnológica ou por deliberação do Comitê de Segurança da Informação.

Art. 41 Os casos omissos e as dúvidas sobre esta Política e seus documentos complementares serão decididos pelo Diretor de Gestão Estratégica, ouvido o Comitê de Segurança da Informação do Cefet/RJ.

Art. 42 Esta Política entra em vigor na data de sua publicação.