SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA

Política de Segurança da Informação e Comunicação do Cefet/RJ

Art. 1° O presente documento tem por objetivo instituir a Política de Segurança da Informação e Comunicação - POSIC no âmbito do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - Cefet/RJ.

CAPÍTULO I
DO ESCOPO

Seção I
Dos Objetivos da Política de Segurança da Informação e Comunicação

Art. 2° A POSIC objetiva garantir a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio das informações produzidas ou custodiadas pelo Cefet/RJ, limitando a exposição ao risco a níveis aceitáveis, a fim de se atingir os objetivos estratégicos desta Instituição.

Art. 3° O Cefet/RJ deverá observar os princípios, objetivos, diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta POSIC, bem como as disposições constitucionais legais e regimentais vigentes.

Art. 4° Integram também a POSIC as normas e os procedimentos complementares destinados à proteção da informação e à regulamentação de sua utilização. Esses dispositivos estão detalhados na página de Legislação sobre segurança da informação e proteção de dados pessoais do Governo Digital, assegurando conformidade com as diretrizes vigentes**.**

Art. 5° As diretrizes de Segurança da Informação consideram, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura do Cefet/RJ.

Seção II
Da Abrangência

Art. 6° As diretrizes, normas complementares e manuais de procedimentos da POSIC do Cefet/RJ aplicar-se-ão à servidores, alunos, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem execute atividades no âmbito desta instituição, ou quem quer que tenha acesso a dados ou informações em seu ambiente.

Parágrafo único. Todos serão responsáveis e deverão estar comprometidos com a segurança da informação.

Art. 7° Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Cefet/RJ deverão atender a esta POSIC.

Art. 8° Esta política também se aplicará, no que couber, ao relacionamento do Cefet/RJ com outros órgãos e entidades públicos ou privados.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 9°. No âmbito da POSIC, considera-se:

I. **Ameaça:** conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;
II. **Ativo:** tudo que tenha valor para a organização, material ou não;
III. **Ativos de informação**: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
IV. **Autenticidade**: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
V. **Capacitação em Segurança da Informação**: Desenvolvimento de aptidões, habilidades e conhecimentos mínimos em Segurança da Informação para o desempenho de suas funções;
VI. **Classificação da informação**: Identificação, dada pelo proprietário da informação, do seu nível de classificação para uso dos controles de proteção necessários;

VII. **Comitê Gestor de Segurança e Tecnologia da Informação (CGSTI)**: órgão colegiado, de caráter permanente, de natureza consultiva e propositiva; e deliberativa exclusivamente sobre as normas internas de segurança da informação, e tem a finalidade de colaborar nas políticas e ações do Cefet/RJ na área de Segurança e Tecnologia da Informação;

VIII. **Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC)**: órgão colegiado deliberativo, de natureza estratégica e caráter permanente, que tem a finalidade de estabelecer políticas e diretrizes para integração dos sistemas que compõem a estrutura de Tecnologia de Informação e Comunicação do Cefet/RJ no âmbito institucional, de aprovar os instrumentos de controles e avaliar ações previstas no Planejamento Estratégico;

IX. **Confidencialidade**: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

X. **Conscientização em Segurança da Informação**: atividade que tem por finalidade orientar sobre o que é Segurança da Informação, 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;

XI. **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Normalmente, envolve procedimentos de autenticação para garantir a segurança;

XII. **ETIR (Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos)**: grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público-alvo específico;

XIII. **Custodiante do ativo de informação**: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante, ou dos ativos de informação que compõem o sistema de informação, que não lhe pertence, mas que está sob sua custódia;

XIV. **Disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

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

XVI. **Documento de natureza pública**: documento relativo ou pertencente à coletividade, de uso comum a todos, do Cefet/RJ conhecido ou sem restrição de acesso a qualquer pessoa;

XVII. **Estrutura de GSI**: grupo responsável pela gestão e execução da Segurança da Informação;

XVIII. **Gerenciamento de operações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporta, satisfazendo os acordos de níveis de serviço;

XIX. **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XX. **Gestão de continuidade dos negócios (GCN)**: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XXI. **Gestão de Riscos de Segurança da Informação (GRSI)**: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

XXII. **Gestão de Segurança da Informação (GSI)**: processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

XXIII. **Gestor da informação**: indivíduo, entidade ou projeto do Cefet/RJ que, no exercício de suas competências, produz informações ou obtém, de fonte externa à instituição, informações de propriedade de pessoa física ou jurídica;

XXIV. **Gestor da unidade administrativa**: servidor nomeado pelo Diretor-Geral como responsável pela gestão administrativa no âmbito do Cefet/RJ;

XXV. **Gestor de Segurança da Informação**: responsável pelas ações de segurança da informação no âmbito do Cefet/RJ;

XXVI. **Gestor dos ativos de informação**: responsável por gerenciar determinado ativo da Informação;

XXVII. **Incidente**: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, 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;

XXVIII. **Incidente de Segurança da Informação**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXIX. **Informação**: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXX. **Infraestrutura de TI**: sistemas e serviços de informação compostos por todo *hardware* e *software* necessários para processar, armazenar e transmitir a informação, ou qualquer combinação desses elementos. O processamento inclui criação, acesso, modificação e destruição da informação. O armazenamento engloba qualquer tipo de mídia na qual a informação esteja armazenada. A transmissão é composta tanto pela distribuição como pelo compartilhamento da informação, por qualquer meio;

XXXI. **Integridade**: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXXII. **Log:** registro de eventos relevantes em um dispositivo ou sistema computacional;

XXXIII. **Não repúdio**: propriedade que assegura que nem o emissor nem o receptor de uma informação possam negar o fato, a autoria, a responsabilização;

XXXIV. **Órgãos de TIC:** Setores de informática ou que desenvolvem tais atividades dos campi e o Departamento de Tecnologia da Informação do Maracanã;

XXXV. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XXXVI. **Recursos criptográficos**: sistema, programa, processo, equipamento isolado ou em rede, que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXXVII. **Risco de Segurança da Informação**: risco potencial associado à exploração de uma ou mais vulnerabilidades, de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXXVIII. **Rótulo**: identificação, física ou eletrônica, da classificação atribuída à informação;

XXXIX. **Segurança da informação (SI)**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XL. **Segurança física e do ambiente**: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XLI. **Sistema estruturante**: sistema com suporte de tecnologia da informação, fundamental e imprescindível para o planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações de Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos ou entidades da administração pública federal, direta ou indireta, e que necessitem de coordenação central;

XLII. **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao Cefet/RJ;

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

XLIV. **Tratamento de incidentes**: consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias;

XLV. **Usuário da informação**: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços e aluno, habilitados pela administração para acessar os ativos de informação do Cefet/RJ.

XLVI. **Vulnerabilidade**: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 10. A POSIC deverá obedecer aos princípios constitucionais, administrativos e do arcabouço legal vigente que regem a Administração Pública nas esferas federal, estadual e municipal.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 11. A Segurança da Informação e Comunicação tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes.

Art. 12. Caberá ao CGSTIC convocar as reuniões de deliberação da POSIC.

Art. 13. Caberá ao Comitê Gestor de Segurança e Tecnologia da Informação instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em Segurança da Informação, buscando também parcerias com outros órgãos e entidades.

Art. 14. As unidades do Cefet/RJ deverão adotar ou utilizar esta POSIC e suas normas complementares como modelos de referência para elaboração dos seus documentos.

Art. 15. A Gestão de Segurança da Informação - GSI deverá apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, à eficácia e a efetividade das atividades de SI.

Parágrafo único. Fica instituído o CGSTI como estrutura de GSI do Cefet/RJ conforme regimento do CGSTI.

Art. 16. Para cada uma das diretrizes constantes das seções deste capítulo poderão ser elaboradas normas específicas, manuais e procedimentos, conforme especialização de cada área do Cefet/RJ.

Seção I

Do Tratamento da Informação

Art. 17. As informações produzidas e custodiadas pela instituição serão classificadas em função do seu grau de confidencialidade, disponibilidade, integridade, prazo de retenção e em políticas elaboradas pelo CGSTI.

Parágrafo único. Os dados pessoais seguirão as classificações e determinações da legislação aplicável e da Política de Proteção de Dados Pessoais da instituição.

Art. 18. A GSI do Cefet/RJ deverá auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da instituição e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 19. É vetado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas ou custodiadas pelo Cefet/RJ.

Parágrafo único. O CGSTI deverá elaborar norma de formas de descarte de informações.

Art. 20. O custodiante do ativo de informação deverá ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único. A não designação pressupõe que o gestor é o próprio custodiante.

Art. 21. Os contratos firmados pelo Cefet/RJ deverão conter cláusulas que determinem a observância da POSIC e suas respectivas normas.

Art. 22. Os usuários deverão ter ciência:

I. das ameaças e preocupações relativas à SI;
II. de suas responsabilidades e obrigações no âmbito desta POSIC.

Art. 23. Todos os usuários do Cefet/RJ deverão ser sensibilizados por meio de processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, com o fim de apoiar esta POSIC.

Art. 24. Todos os usuários deverão difundir e exigir o cumprimento da POSIC, das normas de segurança e da legislação vigente acerca do tema.

Art. 25. O uso de recursos criptográficos interfere na Confidencialidade, Integridade e Autenticidade das informações, sendo, portanto, responsabilidade do CGSTI a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas no Cefet/RJ, em conformidade com as orientações contidas em norma específica.

Art. 26. A estrutura do CGSTI deverá estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Art. 27. As informações produzidas por servidores, colaboradores e prestadores de serviços, no exercício de suas funções, são patrimônio intelectual do Cefet/RJ, sujeitas à política de classificação da informação e não caberá a seus criadores qualquer forma de direito autoral.

Art. 28. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do Cefet/RJ em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica e formal pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Diretor-geral, nos demais casos.

Art. 29. Os acordos com terceiros deverão envolver todas as partes interessadas.

Parágrafo único. Os acordos que concedam o acesso a terceiros poderão incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos, desde que expressamente autorizadas pelo Cefet/RJ.

Seção II

Da Segurança Física e do Ambiente

Art. 30. A Estrutura de GSI deverá estabelecer mecanismos de proteção às instalações físicas e áreas de processamento e armazenamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências internas e externas. As proteções deverão estar alinhadas aos riscos identificados.

Art. 31. O *hardware* responsável pela execução de sistemas de missão crítica deverá estar protegido contra problemas de segurança física, dispondo de recurso de redundância de processador, disco, sistemas elétricos etc., bem como de equipamentos de controle da corrente elétrica (rede estabilizada), temperatura, umidade e acesso físico restrito.

Parágrafo único. Caberá ao CGSTI classificar os sistemas de missão crítica e a sua definição de proteção, considerando a criticidade das informações e os ativos de informação envolvidos nesses sistemas.

Art. 32. A alimentação de energia e refrigeração do ambiente onde se encontram estes sistemas de missão crítica deverão ter o seu pleno funcionamento garantido.

Art. 33. Os ambientes lógicos deverão ser segregados, de modo que o ambiente de produção fique apartado dos demais, e que somente sejam acessados por usuários internos responsáveis pela implantação dos sistemas de informação, sob a responsabilidade do órgão de TIC do Cefet/RJ.

Art. 34. Deverão existir ambientes de homologação/teste separados do ambiente de produção, permitindo que sejam feitos testes em ambiente apropriado, controlado e gerenciado.

Art. 35. A passagem de programas e dados para o ambiente de produção deverá ser controlada de maneira a garantir a integridade e a disponibilidade desse ambiente para sua execução.

Art. 36. Os sistemas de informação que forem transferidos para o ambiente de produção deverão ter seu código-fonte original mantido por um sistema interno de gerenciamento de repositórios de código-fonte.

Art. 37. A segurança da infraestrutura de rede do Cefet/RJ é uma responsabilidade de todos os seus usuários que deverão zelar pela sua preservação e manter conservada da forma que está implantada no *campus*.

Parágrafo único. Qualquer solicitação de mudança ou mudança efetiva deverá ser avaliada pelos órgãos de TIC para aprovação.

Seção III

Da Gestão de Incidentes em Segurança da Informação

Art. 38. Fica instituída a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), composta por servidores efetivos, com capacitação técnica compatível com as atividades da equipe e com atribuições e competências determinadas pela legislação competente e coordenadas pelo DTINF.

Parágrafo único. Todo e qualquer incidente de Segurança da Informação ocorrido no âmbito do Cefet/RJ e demais órgãos correlatos, deverão ser formalmente comunicados através do e-mail do ETIR.

Art. 39. Para evitar ou minimizar os impactos de situações de interrupção dos sistemas de informação e comunicações causados por incidentes de segurança, o ETIR deverá manter um Plano de Gerenciamento de Incidentes, elaborado e alinhado ao Programa de Gestão de Continuidade de Negócios.

Seção IV
Da Gestão de Ativos

Art. 40. Os ativos de informação deverão:

I. ser inventariados e protegidos;
II. ter identificados os seus proprietários e custodiantes;
III. ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
IV. ter a sua entrada e saída nas dependências do Cefet/RJ autorizadas e registradas por autoridade competente;
V. ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de ferramentas que permitam a rastreabilidade dos usos desses ativos;
VI. ser utilizados estritamente dentro do seu propósito, sendo vedado seus usos para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 41. O CGSTI, ou comitê especialmente designado, deverá criar, gerir e avaliar critérios de tratamento, de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 42. Os recursos tecnológicos, instalações de infraestrutura e os sistemas de informação e demais ativos do Cefet/RJ deverão ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 43. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizado, deverá ser condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 44. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

Seção V

Da Gestão do Uso dos Recursos Operacionais e de Comunicações

Art. 45. No que diz respeito ao uso de recursos como inteligência artificial (IA), Internet das Coisas (IoT), correio eletrônico, acesso à internet, redes sociais, computação em nuvem, e outros recursos ligados diretamente à Tecnologia da Informação, o CGSTI deverá propor ao CGTIC normas para regulamentação.

Art. 46. A Estrutura de GSI deverá estabelecer normas adequadas, relacionados à SI, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiem, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do Cefet/RJ.

Art. 47. Deverá haver, pelo menos, um responsável pelas questões de segurança dos serviços de TI, na unidade onde eles estiverem instalados.

Art. 48. Os servidores *web* deverão ser configurados, de modo que permitam a utilização de tecnologias de autenticação e criptografia, que possam garantir a integridade, o sigilo e a autenticidade das informações, cabendo ao CGSTI definir e pôr em prática as medidas que garantam a segurança de tais equipamentos, de forma a não comprometer a segurança das redes internas e externas à instituição.

Art. 49. O DTINF deverá propor procedimentos e mecanismos de autenticação que permitam determinar a titularidade de todos os acessos à internet feitos pelos usuários dentro da instituição para o CGSTI avaliar.

Seção VI

Do Controle de Acesso

Art. 50. Do controle de acesso às informações:

I. é dever do gestor da área responsável pela informação manter os dados atualizados e propor normas de acesso a elas;
II. deverão estabelecer controles de perfis, permissões e procedimentos necessários para a salvaguarda da SI.

Art. 51. Os ambientes críticos do Cefet/RJ deverão ter o seu acesso restrito por senhas seguras, conforme norma específica de senhas, ou outros mecanismos de segurança apropriados, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pelo DTINF.

Art. 52. Deverão ser registrados eventos relevantes, previamente definidos na Política de Gestão de Registros (Logs) de Auditoria, para a segurança e o rastreamento de acesso às informações.

Art. 53. Deverão ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 54 Os usuários do Cefet/RJ são responsáveis por todos os atos autenticados, sejam digitais ou físicos.

Art. 55. A identificação do usuário, qualquer que seja o meio e a forma (crachá, assinatura, usuário e senha, voz, foto etc.), deverá ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 56. A autorização, o acesso e o uso das informações e dos recursos computacionais deverão ser controlados e limitados ao necessário, considerando as atribuições de cada usuário.

Parágrafo único. A ampliação dos limites de acesso dependerá de prévia autorização do gestor da área responsável pela informação.

Art. 57. Todos os sistemas de informação do Cefet/RJ, automatizados ou não, deverão ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

Art. 58. Os privilégios de acesso às informações e aos recursos computacionais deverão ser adequados imediatamente após a mudança nas atribuições do usuário.

Parágrafo único. Os privilégios de acesso às informações e aos recursos computacionais deverão ser cancelados, em caso de desligamento do Cefet/RJ, ou suspensos, em casos de afastamentos e afins.

Art. 59. Os sistemas estruturantes deverão possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:

I. ao acesso às suas bases de dados;
II. à extração, carga e transformação de dados;
III. aos serviços acessíveis via linguagem de programação.

Art. 60. Os sistemas estruturantes deverão possuir mecanismos para:

I. revogar as concessões e desativar as contas de acesso do usuário nos casos de afastamento permanente.
II. criação automática de logs de acessos, com informações suficientes para inequívoca identificação de qual usuário fez o acesso e as transações críticas executadas.
III. bloquear as contas de acesso dos usuários nos casos de afastamento temporário.

Art. 61. É responsabilidade da chefia da unidade administrativa que possui recursos compartilhados entre a equipe, incluindo servidores ou outro tipo de colaborador, informar mudanças para configuração adequada dos perfis de acesso.

Seção VII

Da Gestão de Riscos

Art. 62. Caberá aos responsáveis pelos ativos de informação estabelecer processos de Gestão de Riscos de Segurança da Informação – GRSI que possibilitem identificar ameaças e reduzir suas vulnerabilidades, assim como reduzir os impactos de eventuais incidentes com eles.

Art. 63. A GRSI é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação, levando em consideração o planejamento, execução, análise crítica e melhoria da segurança da informação no Cefet/RJ.

Seção VIII

Da Gestão de Continuidade

Art. 64. Entende-se como Gestão da Continuidade do Negócio o processo que fornece uma estrutura para que a organização desenvolva uma resiliência que a possibilite responder de forma efetiva aos ataques sofridos por ameaças potenciais identificadas, salvaguardando os seus interesses.

Art. 65. As normas e procedimentos para implantação e gestão da continuidade do negócio serão definidos na Política de Gestão de Continuidade - PGCN do Cefet/RJ.

Art. 66. Os recursos contemplados no Plano de Continuidade do Negócio – PCN devem ser preferencialmente redundantes e mantidos em condições técnicas e ambientais determinadas pela área técnica responsável, de forma a garantir a sua máxima disponibilidade e a continuidade de suas atividades críticas ainda que em caso de incidentes

Seção IX

Da Auditoria e Conformidade

Art. 67. O cumprimento desta política deverá ser avaliado periodicamente por meio de verificações de conformidade.

Art. 68. Todos os usuários estão sujeitos à auditoria pela utilização dos recursos do Cefet/RJ.

Art. 69. As unidades responsáveis pela custódia dos ativos de informação, ou definidas como competentes, deverão realizar periodicamente auditoria, monitoramento e verificação da aplicação desta POSIC.

CAPÍTULO V
DAS PENALIDADES

Art. 70. Ações que violem a POSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SI serão devidamente apuradas por processo administrativo e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPOSABILIDADES

Art. 71. Compete a Direção-geral do Cefet/RJ, através do CGSTI, comprometer-se em zelar pela proteção de todos os seus ativos de informação, conforme art. 17 do decreto nº 9.637 de 26 de dezembro de 2018 da Presidência da República.

Art. 72. Caberá ao CGSTI as competências e responsabilidades descritas em seu regimento.

Art. 73. Caberá às diretorias:

I. conscientizar os usuários sob sua supervisão em relação aos conceitos e as práticas de SI;
II. incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SI;
III. tomar as medidas administrativas necessárias para que sejam aplicadas 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;
V. manter lista atualizada dos ativos de informação sob sua responsabilidade, com seus respectivos gestores.

Art. 74. Caberá aos terceiros e fornecedores, conforme previsto em contrato:

I. tomar conhecimento desta POSIC;
II. observar, no exercício de suas atividades, a íntegra desta POSIC;
III. fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação, objetos do contrato;
IV. fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 75. Caberá aos usuários:

I. conhecer e cumprir todas as políticas, normas e procedimentos relacionados à SI;
II. comunicar formalmente, via sistema de chamados ou e-mail, os incidentes que afetam a segurança dos ativos de informação ao DTINF.
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 e Comunicação (POSIC) quanto da Segurança da Informação (SI) no âmbito do CEFET

CAPÍTULO VII
DOS PROCEDIMENTOS DE ATUALIZAÇÃO E TRANSIÇÃO

Art. 76. Esta POSIC, bem como os documentos gerados a partir dela, deverão ser revisados anualmente, ou por deliberação do CGTIC.

Parágrafo único. O CGSTI formalizará a proposta de revisão da POSIC, a qual deve ser, sucessivamente, apreciada e aprovada pelo CGTIC.

Art. 77. O CGSTI deverá elaborar e propor as suas normas e procedimentos de SI e submeter ao CGTIC.

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

PUBLICADA. CUMPRA-SE