MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
CONSELHO DIRETOR

# RESOLUÇÃO Nº 45, DE 14 DE SETEMBRO DE 2018.

Aprova a Política de Segurança Cibernética do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – CEFET/RJ.

O PRESIDENTE DO CONSELHO DIRETOR DO CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA, no uso de suas atribuições, e em obediência à deliberação do Conselho Diretor, em sua 7ª Sessão Ordinária, realizada em 14 de setembro de 2018,

**R E S O L V E:**

**Art. 1º** – Aprovar a Política de Segurança Cibernética do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – CEFET/RJ, conforme anexo.

**Art. 2º** – Esta Resolução entra em vigor na data de sua assinatura.

CARLOS HENRIQUE FIGUEIREDO ALVES

# POLÍTICA DE SEGURANÇA CIBERNÉTICA DO CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA - CEFET/RJ

## Capítulo I

## DAS DISPOSIÇÕES GERAIS

**Art.1º** A Política de Segurança Cibernética visa estabelecer requisitos mínimos para a aplicação da Segurança Cibernética no Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – Cefet/RJ.

**Art.2º** Compreende-se por Segurança Cibernética a proteção aos sistemas de informação (*hardwares*, *softwares* e infraestruturas associadas), aos dados neles contidos e aos serviços que disponibilizam, contra o acesso não autorizado, prejuízos ou uso indevido por meio de ferramentas, políticas, conceitos de segurança, salvaguardas, orientações, abordagens de gestão de risco, ações, treinamentos, melhores práticas, seguros e tecnologias.

## Capítulo II

## DA FUNDAMENTAÇÃO NORMATIVA E LEGAL

**Art 3º** Esta política foi elaborada com base na ABNT NBR-ISO/IEC-27001:2013 que trata de dos Requisitos para Sistemas de Gestão de Segurança da Informação, ABNT NBR-ISO/IEC-27002:2013 que trata do Código de prática para a Gestão de Segurança da Informação, ABNT NBR ISO/IEC-22301:2013, que trata da Gestão de Continuidade de Negócios; ABNT NBR ISO/IEC-27005:2008, que trata de Gestão de Riscos de Segurança da Informação; ABNT NBR ISO/IEC-27014:2013 que trata da Governança de Segurança da Informação; Norma NBR ISO/IEC 27017:2016 que trata do Código de prática controles segurança da informação para serviços em nuvem; **Norma Complementar nº 03/IN01/DSIC/GSIPR** que trata das Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal e Resolução BC nº 4.658/2018.

## Capítulo III

## DOS OBJETIVOS

**Art.4º** O Cefet/RJ deve assegurar que o gerenciamento de riscos em TI disponha, no tocante à continuidade de negócios, sobre:

I - o tratamento dos incidentes relevantes relacionados com o ambiente cibernético;

II - os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados, abrangendo cenários que considerem o reestabelecimento da operação normal do Cefet/RJ; e

III - os cenários de incidentes considerados nos testes de continuidade de negócios.

**Art.5º** Os procedimentos adotados pelo Cefet/RJ para gerenciamento de riscos em TI devem contemplar, no tocante à continuidade de negócios:

I - o tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços relevantes de processamento e armazenamento de dados;

II - o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos.

**Art.6º** O Cefet/RJ deve instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da Segurança Cibernética, do plano de ação e de resposta a incidentes, incluindo:

I - a definição de processos, testes e trilhas de auditoria;

II - a definição de métricas e indicadores adequados; e

III - a identificação e a correção de eventuais deficiências.

## Capítulo IV

## DAS DEFINIÇÕES

**Art.7º** Para fins desta política, considera-se a definição dos seguintes termos:

I - **Auditoria**: ato de verificar e avaliar os sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

II - **Autenticação**: ato de confirmar sobre autenticidade de algo ou alguém, ou seja, uma garantia de que qualquer alegação de ou sobre um determinado objeto é verdadeira;

III - **Confidencialidade**: propriedade de que a informação não esteja disponível ou seja revelada a pessoa física, sistema, órgão ou entidade, caso não seja autorizado ou credenciado;

IV - **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por qualquer pessoa física ou determinado sistema, órgão ou entidade;

VI - **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

VII - **Softwares maliciosos**: programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

## Capítulo V

## DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

**Art.8º** Esta Política de Segurança Cibernética foi formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

### Seção I

### Da Implementação da Política de Segurança Cibernética

**Art.9º** A Política de Segurança Cibernética, deverá contemplar, no mínimo:

I - os objetivos de segurança cibernética do Cefet/RJ;

II - os procedimentos e os controles adotados para reduzir a vulnerabilidade do Cefet/RJ a incidentes e atender aos demais objetivos de segurança cibernética;

III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Cefet/RJ;

V - as diretrizes para:

a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços ao Cefet/RJ que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais do Cefet/RJ;

c) a classificação dos dados e das informações quanto à relevância; e

d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

VI - os mecanismos para disseminação da cultura de segurança cibernética no Cefet/RJ, incluindo:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações a usuários sobre precauções na utilização de serviços providos pelo DTINF; e

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

VII – as iniciativas para compartilhamento de informações sobre os incidentes relevantes.

**§ 1º** Na definição dos objetivos de segurança cibernética referidos no inciso I do caput, deve ser contemplada a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

**§ 2º** Os procedimentos e os controles de que trata o inciso II do caput devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

**§ 3º** Os procedimentos e os controles citados no inciso II do caput devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação e na adoção de novas tecnologias empregadas nas atividades do Cefet/RJ.

**§ 4º** O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, citados no inciso IV do caput, devem abranger inclusive informações recebidas de empresas prestadoras de serviços ao Cefet/RJ.

**§ 5º** As diretrizes de que trata o inciso V, alínea "b", do caput devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pelo próprio Cefet/RJ.

## Seção II

## Do Plano de Ação e de Resposta a Incidentes

**Art.10** O Cefet/RJ deve estabelecer plano de ação e de resposta a incidentes visando à implementação da segurança cibernética.

**Parágrafo único** - O plano mencionado no caput deve abranger, no mínimo:

I - as ações a serem desenvolvidas pelo Cefet/RJ para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes de segurança cibernética;

II - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizadas na prevenção e na resposta a incidentes, em conformidade com as diretrizes da segurança cibernética; e

III - a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

**Art.11** O CGTIC deverá designar o servidor ou equipe responsável pelo planejamento da Segurança Cibernética na instituição e pela execução do plano de ação e de resposta a incidentes.

**Parágrafo único** - O servidor ou a equipe mencionada no caput podem desempenhar outras funções no Cefet/RJ, desde que não haja conflito de interesses.

**Art.12** O CGTIC deve solicitar ao responsável pelo exposto no Art 10 um relatório anual sobre a implementação do plano de ação e de resposta a incidentes, mencionado no art. 9º, com data-base de 31 de dezembro.

**§ 1º** O relatório de que trata o caput deve abordar, no mínimo:

I - a efetividade da implementação das ações descritas no art. 8º, parágrafo único, inciso I;

II - o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes descritos no art. 8º, parágrafo único, inciso II;

III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

**§ 2º** O relatório mencionado no caput deve ser:

I - submetido ao Comitê de Governança, Riscos e Controles (CGRC) e ao Comitê de Governança de Tecnologia da Informação (CGTIC);

II – apresentado ao Conselho Diretor (CODIR) e aprovado até 31 de março do ano seguinte ao da data-base.

**Art.13** As normativas de segurança cibernética derivadas do planejamento e o plano de ação e de resposta a incidentes, mencionados no art. 8º, devem ser aprovados pelo CGTIC.

**Parágrafo único** - Os documentos do *caput* devem ser documentados e revisados anualmente.

**Art.14** Esta política entra em vigor na data de sua publicação.