



MINISTÉRIO DA EDUCAÇÃO  
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca  
Direção-Geral

**PORTARIA Nº 1410/CEFET-RJ, DE 23 DE SETEMBRO DE 2025**

**O Diretor-Geral do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca**, nomeado pela Portaria MEC nº 146, de 26/02/2025, publicada no DOU de 28/02/2025, Seção 2, pág. 18, no uso de suas atribuições e considerando a aprovação do Comitê de Governança, Riscos e Controles, na reunião de 09/09/2025,

**RESOLVE**

Art. 1º Aprovar e tornar público o Regulamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), no âmbito do Cefet/RJ.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

**Publicação:** [Transparência Ativa](#) em 23 de setembro de 2025

**Documento assinado eletronicamente sob [fundamentação](#), por:**  
MAURICIO SALDANHA MOTTA

**Data da Assinatura:**  
23 de setembro de 2025 as 17:00 (America/Sao\_Paulo)

**Tipo de Documento:**  
Portaria



Autenticidade



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

## **Regulamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos**

Regulamenta o funcionamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)

O DIRETOR-GERAL DO CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA, designado pela Portaria MEC nº 146, de 26/02/2025, publicada no D.O.U. de 28/02/2025, Seção 2, pág. 18, no uso de suas atribuições legais,

**RESOLVE:**

### **Seção I**

#### **Da criação e missão**

**Art. 1º** Instituir e regulamentar o funcionamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), no âmbito do Cefet/RJ, subordinada ao Comitê de Segurança da Informação (CSI), composta por servidores efetivos, com capacitação técnica compatível com as atividades da equipe e com as diretrizes estabelecidas na Política de Segurança da Informação (POSIC) da instituição.

§ 1º Não existirá um grupo dedicado exclusivamente às funções de prevenção, tratamento e resposta a incidentes cibernéticos. Os membros da ETIR desempenharão, além de suas funções regulares, as atividades elencadas neste Regulamento.

§ 2º A participação na ETIR será considerada prestação de serviço público relevante, não remunerada.

**Art. 2º** A ETIR do Cefet/RJ tem como missão prioritária planejar, coordenar e executar atividades de prevenção, tratamento e resposta a incidentes cibernéticos, monitorar as redes, seus serviços e suas vulnerabilidades, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, preservando, assim, os dados, as informações e a infraestrutura de rede da instituição.

Parágrafo único. A ETIR atenderá diretamente todas as unidades acadêmicas, setores administrativos e solicitantes externos que registrarem eventos identificados como incidentes cibernéticos.

## Seção II

### Definições

**Art. 3º** Para os fins deste regulamento, considera-se:

- I — EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) - grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade.
- II — INCIDENTE CIBERNÉTICO - ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistemas de informação ou das informações processadas, armazenadas ou transmitidas por esses sistemas. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que configure violação de norma, política de segurança, procedimento de segurança ou política de uso.
- III — REDE DE DADOS DO CEFET/RJ - Conjunto de infraestrutura física e lógica que possibilita a transmissão, o armazenamento e o processamento de informações no âmbito do CEFET/RJ.
- IV — PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO - Documento estratégico que descreve os procedimentos e ações a serem adotados para identificar, mitigar, responder e recuperar-se de incidentes cibernéticos, com o objetivo de minimizar impactos operacionais e reputacionais.
- V — POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - Documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta ou indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.
- VI — 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.
- VII — TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS - Consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade das operações, preservar evidências e emitir as notificações necessárias.
- VIII — AÇÕES PREVENTIVAS - medidas adotadas de forma antecipada para reduzir a probabilidade de ocorrência de incidentes cibernéticos ou minimizar seus impactos caso ocorram;
- IX — AÇÕES DE CONSCIENTIZAÇÃO E CAPACITAÇÃO - atividades voltadas para educar e treinar a comunidade acadêmica e administrativa do Cefet/RJ sobre boas práticas e responsabilidades relacionadas à segurança da informação.
- X — Comitê de Segurança da Informação - grupo de pessoas responsáveis por assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.
- XI — Solicitantes externos: indivíduos, organizações ou instituições sem vínculo direto com o Cefet/RJ que demandem suporte da ETIR em casos de incidentes cibernéticos que afetem os serviços ou sistemas da instituição.

**Art. 4º** A ETIR tem por escopo de atuação a prevenção da ocorrência de incidentes de segurança da informação, a mitigação de riscos relacionados à segurança da informação e a realização de ações reativas que incluem, mas não se limitam a:

- I — Receber, analisar e responder às notificações e às atividades relacionadas a incidentes de segurança em redes de computadores.
- II — Desenvolver as atividades de prevenção, tratamento e resposta a incidentes de segurança da informação.
- III — Notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov) sobre a ocorrência de qualquer incidente de segurança, seguindo os formatos e procedimentos estabelecidos pelo CTIR Gov; e
- IV — Trocar informações acerca de segurança da informação com as demais equipes de prevenção, tratamento e resposta a incidentes cibernéticos.

**Art. 5º** A comunicação de incidentes cibernéticos na rede de dados do Cefet/RJ deverá ser realizada pelo Sistema de Chamados: <https://chamados.cefet-rj.br/open.php>, na opção Incidentes de Segurança, ou pelo e-mail [segur@cefet-rj.br](mailto:segur@cefet-rj.br).

**Art. 6º** A ETIR trabalhará de forma autônoma e poderá recomendar e/ou realizar os procedimentos a serem executados ou as medidas de recuperação durante os incidentes cibernéticos.

Parágrafo único. A ETIR contará com o apoio da alta administração e dos setores da organização, dependendo da natureza do incidente e da criticidade, a fim de participar do processo de tomada de decisão sobre quais medidas deverão ser adotadas.

**Art. 7º** A estrutura organizacional da ETIR será composta pelos seguintes representantes do Cefet/RJ:

- I — o gestor do Departamento de Tecnologia da Informação;
- II — o gestor de segurança da informação;
- III — o encarregado pela proteção de dados pessoais;
- IV — representante(s) da Divisão de Infraestrutura de Informação - DINFO;
- V — representante(s) da Divisão de Estratégia e Governança em TI - DIGTI; e
- VI — representante(s) da Divisão de Desenvolvimento e Manutenção de Sistemas - DIDMS.

Parágrafo único. O Gestor de Segurança da Informação atuará como coordenador da equipe, sendo responsável por representá-la e responder por ela, gerenciar as atividades de seus membros, bem como coordenar metodologias e procedimentos internos.

**Art. 8º** A ETIR do Cefet/RJ desempenhará os seguintes serviços:

- I — tratamento de vulnerabilidades;
- II — tratamento de incidentes cibernéticos;
- III — emissão de alertas e advertências;
- IV — anúncios e disseminação de informações relacionadas à segurança;
- V — detecção de intrusão; e
- VI — outras atividades determinadas pelo CSI.

Parágrafo único. conforme a necessidade da ETIR, outros serviços poderão ser oferecidos.

**Art. 9º** São atribuições da ETIR do Cefet/RJ:

- I — Monitorar e registrar atividades suspeitas ou incidentes cibernéticos nas redes de dados do Cefet/RJ;
- II — Diagnosticar e classificar incidentes de segurança, definindo suas causas e impactos;
- III — Executar ações de contenção, erradicação e recuperação para mitigar os danos de incidentes de segurança;
- IV — Elaborar relatórios e pareceres técnicos sobre os incidentes tratados e suas respectivas resoluções;
- V — Desenvolver e manter atualizado o plano de resposta a incidentes de segurança do Cefet/RJ;
- VI — Identificar, registrar, analisar e mitigar incidentes de segurança relacionados às redes de dados e sistemas computacionais do Cefet/RJ;
- VII — Implementar ações preventivas e corretivas para a melhoria contínua da segurança da informação;
- VIII — Propor normas, políticas e procedimentos que garantam a integridade, confidencialidade e disponibilidade dos dados institucionais;
- IX — Promover ações de conscientização e capacitação para a comunidade acadêmica e administrativa sobre boas práticas de segurança digital; e
- X — Atuar em articulação com outras instituições, quando necessário, para garantir a resposta coordenada a incidentes de segurança cibernética.

**Art. 10** A ETIR do Cefet/RJ se reunirá em caráter ordinário sempre que necessário, por proposição fundamentada de um ou mais de seus membros.

**Art. 11** A ETIR deverá se integrar às tecnologias, padrões, procedimentos e processos estabelecidos pelo CISC Gov.br, observando os normativos do Gabinete de Segurança Institucional da Presidência da República.

**Art. 12** O presente Regulamento deve ser lido em conjunto com as obrigações previstas nas referências legais e normativas, e suas atualizações.

**Art. 13** Este Regulamento deverá ser revisado, no máximo, a cada dois anos, quando houver alteração de legislação ou mediante solicitação do Comitê de Segurança da Informação (CSI).

**Art. 14** As atribuições constantes neste regulamento deverão ser exercidas com fiel observância das normas vigentes.

**Art. 15** Casos omissos a este regulamento no contexto das atribuições e funcionamento da ETIR serão decididos pelo Diretor de Gestão Estratégica, ouvido o Comitê de Governança Digital (CGD).

**Art. 16** Este regulamento entra em vigor na data de sua publicação.