MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO
Av. Jorge Amado, 1551 – Loteamento Garcia, Bairro Jardins - CEP 49025-330 – Aracaju/SE
Fone: (79) 3711-3140 – E-mail: dti@ifs.edu.br

DELIBERAÇÃO Nº 02/2017/CGTIC/IFS

Aprova o regulamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Instituto Federal de Sergipe.

O PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, faz saber que, no uso das atribuições legais que lhe confere a Lei nº 11.892 de 29 de dezembro de 2008, em conformidade com a Portaria IFS nº 1.039 de 28/04/2014 e 1.339 de 05/06/2014, e considerando a Instrução Normativa GSI Nº 1, de 13 de junho de 2008, Norma Complementar nº 05/IN01/DSIC/GSIPR, Norma Complementar nº 08/IN01/DSIC/GSIPR, Norma Complementar nº 21/IN01/DSIC/GSIPR e a 1ª reunião ordinária do Comitê Gestor de Tecnologia da Informação e Comunicação realizada em 20/02/2017;

RESOLVE:

I – APROVAR o regulamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe - IFS.

II - Esta Deliberação entra em vigor nesta data.

Aracaju, 20 de fevereiro de 2017.

Ailton Ribeiro de Oliveira
Presidente do CGTIC/IFS

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
13/02/2017	1.0	Instrução Normativa que dispõe sobre o Regulamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR no Instituto Federal de Sergipe	Fernando Lucas de Oliveira Farias (DTI) e Demair de Sá Ramos (COSEG)
14/02/2017	1.1	Revisão do regulamento pelos Coordenadores Sistêmicos da DTI em reunião extraordinária	Coordenadores Sistêmicos da DTI
15/02/2017	1.2	Revisão do regulamento pelos Coordenadores e servidores de TI dos campi em reunião extraordinária	Coordenadores e servidores de TI dos Campi
20/02/2017	1.3	Aprovação da Instrução Normativa pelos membros do Comitê Gestor de TI em reunião ordinária	Comitê Gestor de TI

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO
Av. Jorge Amado, 1551 – Loteamento Garcia, Bairro Jardins - CEP 49025-330 – Aracaju/SE
Fone: (79) 3711-3140 – E-mail: dti@ifs.edu.br

INSTRUÇÃO NORMATIVA **DTI** Nº 02, DE 20 DE FEVEREIRO DE 2017.

Dispõe sobre o regulamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Instituto Federal de Sergipe.

O PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, faz saber que, no uso das atribuições legais que lhe confere a Lei nº 11.892 de 29 de dezembro de 2008, em conformidade com a Portaria IFS nº 1.039 de 28/04/2014 e 1.339 de 05/06/2014, e considerando a Instrução Normativa GSI Nº 1, de 13 de junho de 2008, Norma Complementar nº 05/IN01/DSIC/GSIPR, Norma Complementar nº 08/IN01/DSIC/GSIPR, Norma Complementar nº 21/IN01/DSIC/GSIPR e a 1ª reunião ordinária do Comitê Gestor de Tecnologia da Informação e Comunicação realizada em 20/02/2017;

RESOLVE:

Art. 1º. Instituir e regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR do Instituto Federal de Sergipe – IFS.

Art. 2º. A ETIR do IFS tem como missão prioritária planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura da instituição.

Parágrafo único. É incumbência da ETIR Central e ETIR Descentralizadas (*Campi*) atuar de forma proativa com o objetivo de minimizar o risco de que vulnerabilidades sejam exploradas por ameaças e venham a comprometer o negócio da Instituição, a fim de contribuir para o adequado funcionamento dos serviços de Tecnologia da Informação e Comunicação – TIC no assessoramento das atividades administrativas, ensino, pesquisa e extensão.

CAPÍTULO I
DAS DEFINIÇÕES

Art. 3º. Para os fins desta Instrução Normativa considera-se:

I – Agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II – Artefato malicioso: É qualquer programa de computador ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III – Comunidade ou Público Alvo: É o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV – CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicação – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI – Incidentes de segurança: É qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII – Serviço: É o conjunto de procedimentos estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VIII – Tratamento de Incidentes de Segurança em Redes Computacionais: É o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX – Vulnerabilidade: É qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 4º. As diretrizes estabelecidas nesta instrução normativa deverão ser aplicadas na Reitoria e em todos os *Campi* do IFS.

CAPÍTULO III
DA COMUNIDADE OU PÚBLICO ALVO

Art. 5º. São considerados como comunidade ou público alvo da Rede Corporativa de Computadores e Sistemas do Instituto Federal de Sergipe, os seguintes usuários:

I. Todos os servidores e colaboradores que exercem suas atividades no âmbito do IFS;

II. Demais equipes tratamento e resposta a Incidentes em Redes Computacionais da Administração Pública Federal;

III. CTIR GOV;

IV. Órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos ou convênios com o Instituto Federal de Sergipe para o compartilhamento de informações;

V. Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.

CAPÍTULO IV
DA COMUNICAÇÃO

Art. 6º. A comunicação dos incidentes de segurança em redes de computadores no âmbito do IFS à ETIR será realizada através dos seguintes canais:

I. E-mail para o endereço abuse@ifs.edu.br;

II. Abertura de chamado através da plataforma GLPI, devendo assinalar o tipo como "Incidente" na requisição do serviço;

III. Pessoalmente, em casos emergenciais;

IV. Ferramental tecnológico, eventos detectados pelo monitoramento da ETIR Central ou as ETIR Descentralizadas (*Campi*).

Parágrafo único. O agente responsável pela ETIR Central deve comunicar a ocorrência de incidentes de segurança em redes de computadores ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV, conforme procedimentos a serem definidos pelo próprio CTIR GOV, com vistas a permitir soluções integradas para Administração Pública Federal – APF, bem como a geração de estatísticas, conforme orienta a Norma Complementar nº 5/IN01/DSIC/GSIPR.

Art.7º. O agente responsável pela ETIR Central deverá interagir com forças policiais especializadas e com o judiciário, conforme os casos aplicáveis e a natureza dos incidentes.

Art. 8º. A ETIR Central será responsável por emitir informativos sobre novas vulnerabilidades e atualizações utilizando os seguintes meios de comunicação: e-mails informativos, publicações na intranet, além de *feedback* dos incidentes tratados.

Art. 9º. A ETIR Central deverá notificar de imediato o CTIR GOV através do envio de e-mail para "ctir@ctir.gov.br" com assunto: "[IFS]" e o "tipo de incidente", conforme estabelecem o item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR e o item 6 da Norma Complementar nº 08/IN01/DSIC/GSIPR nos seguintes casos:

I. Abuso de sítios (desfiguração, injeção de links/códigos – *spamdexing*, erros de código, *cross site scripting*, abuso de fórum ou livros de visita, etc);

II. Inclusão remota de arquivos (*remote file inclusion* -RFI) em servidores web;

III. Uso abusivo de servidores de e-mail;

IV. Hospedagem ou redirecionamento de artefatos ou códigos maliciosos;

V. Ataques de negação de serviço;

VI. Uso ou acesso não autorizado a sistema ou dados;

VII. Varredura de portas;

VIII. Comprometimento de computadores ou redes;

IX. Desrespeito à política de segurança ou uso inadequado dos recursos de Tecnologia da Informação (TI);

X. Ataques de engenharia social – *phising*;

XI. Cópia e distribuição não autorizada de material protegido por direitos autorais;

XII. Uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.

Parágrafo único. Nos casos de *phising* recebido por e-mail, solicita-se que além do texto da mensagem, sejam enviados os cabeçalhos completos para que se proceda, dentre outras coisas, à notificação do servidor de e-mail comprometido.

Art. 10. A ETIR Central deverá, conforme estabelece o item 8.5 da Norma Complementar nº 08/IN01/DSIC/GSIPR, havendo indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, além de comunicar ao CTIR GOV, acionar as autoridades policiais competentes para a adoção dos procedimentos legais necessários. Neste caso, deverá observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia e priorizar a continuidade dos serviços da ETIR e da missão institucional do IFS.

CAPÍTULO V
DO MODELO DE IMPLEMENTAÇÃO

Art. 11. O modelo de implementação no qual a ETIR do IFS se baseia é o "Modelo 4 – Combinado ou Misto", descrito na subseção 7.4 na Norma Complementar nº 5 da Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República.

Parágrafo único. O Modelo Combinado ou Misto trata-se da junção dos modelos Descentralizado e Centralizado. Neste modelo existirá uma ETIR Central na Reitoria e ETIR Descentralizadas (*Campi*) distribuídas pelos *campi* do IFS.

Art. 12. A ETIR Central será constituída pelo Coordenador de Segurança da Informação (Presidente) e terá como membros servidores da Coordenadoria de Infraestrutura e Manutenção de Redes – COIMR, Coordenadoria de Sistemas de Informação – CSI e Coordenadoria de Segurança da Informação – COSEG, bem como as seguintes atribuições:

I. Criar estratégias, gerenciar as atividades e distribuir as tarefas entre as ETIR Descentralizadas (Campi);

II. Responsável pela assessoria técnica nas respostas a incidentes de segurança em redes e sistemas;

III. Atuar em grupo de trabalho instituído pelo Comitê de Segurança da Informação juntamente com representantes da área afetada, quando o incidente envolver, recursos de TI e ativos de informação;

IV. Investigar, diagnosticar e registrar os incidentes de segurança em redes;

V. Prover o tratamento do incidente de segurança, quando cabível;

VI. Reportar ao Comitê de Segurança da Informação o incidente e as providências tomadas, podendo propor medidas de prevenção a futuros incidentes;

Art. 13. As ETIR Descentralizadas nos *campi* serão constituídas pelo Coordenador de Tecnologia da Informação (Presidente) e terá como membros os demais servidores da área de TI em exercício na Coordenadoria de Tecnologia da Informação – CTI de cada unidade, bem como as seguintes atribuições:

I. Implementar as estratégias e exercer suas atividades em seus respectivos *campi*, conforme estruturado pela ETIR Central;

II. Ser responsável pela assessoria técnica nas respostas a incidentes de segurança na Rede Computacional de suas unidades;

III. Atuar em grupo de trabalho instituído pelo Comitê de Segurança da Informação em conjunto com representantes da área afetada, quando o incidente envolver recursos de TI e ativos de informação em seu campus;

IV. Investigar, diagnosticar e registrar os incidentes em segurança de Redes;

V. Prover o tratamento do incidente de segurança, quando cabível;

VI. Reportar à ETIR Central o incidente e as providências tomadas, podendo propor medidas de prevenção a futuros incidentes.

CAPÍTULO VI
DA ESTRUTURA ORGANIZACIONAL

Art. 14. A ETIR Central e as ETIR Descentralizadas (Campi) ficarão subordinadas à Coordenadoria de Segurança da Informação – COSEG da instituição.

Art. 15. Para que sejam efetivas em sua missão, as ETIR Central e Descentralizadas (*Campi*) terão competência para solicitar informações e providências das empresas contratadas, prestadoras de serviços de TI, atuando como moderadoras e Coordenadoras dos Serviços, caso necessário.

Art. 16. Serão definidos em portaria o agente responsável, os membros titulares e substitutos em cada ETIR.

Art. 17. Compete ao Agente Responsável pela ETIR:

I. Dimensionar a ETIR, conforme as necessidades institucionais;

II. Submeter a indicação dos membros da ETIR e respectivos substitutos à aprovação do Comitê Gestor de Segurança da Informação ou autoridade equivalente;

III. Coordenar as atividades da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV. Interagir com organismos externos de respostas a incidentes, principalmente o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV;

V. Comparecer as reuniões do Comitê de Segurança da Informação e Comunicações.

Art. 18. Compete aos membros da ETIR e aos substitutos, quando necessário:

I. Prestar os serviços aos quais a ETIR se propõe a fornecer;

II. Definir e documentar a metodologia e os procedimentos internos para o tratamento e resposta aos incidentes;

III. Criar estratégias de resposta a incidentes de rede, elaborar procedimentos de resposta para incidentes previamente conhecidos, gerenciar e atribuir as atividades para a ETIR Descentralizada (*Campi*);

IV. Auxiliar o Gestor de Segurança da Informação e Comunicações na tomada de decisões;

V. Assegurar que os incidentes na Rede de Computadores do Instituto Federal de Sergipe sejam monitorados;

VI. Adotar procedimentos para assegurar que os usuários comuniquem incidentes de segurança da informação e comunicações, bem como obtenham informações acerca das ações adotadas;

VII. Auxiliar em treinamentos relacionados à Segurança da Informação e Comunicação no que se refere à prevenção e combate a incidentes em redes computacionais;

VIII. Recolher tempestivamente as provas quando da ocorrência de um incidente de rede computacional;

IX. Executar uma análise crítica sobre os registros de falha para assegurar que as mesmas foram satisfatoriamente resolvidas;

X. Investigar as causas dos incidentes nas redes computacionais e sistemas de informação;

XI. Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

CAPÍTULO VII
DA AUTONOMIA

Art. 19. A ETIR Central e as ETIR Descentralizadas (*Campi*) terão autonomia completa podendo conduzir o seu públivo alvo ou comunidade para realizar ações ou medidas necessárias para reforçar a resposta ou a postura da instituição na recuperação de incidentes de segurança.

Art. 20. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem aguardar pontualmente pela aprovação de níveis superiores de gestão, visando mitigar eventuais propagações de danos.

CAPÍTULO VIII
DOS SERVIÇOS PRESTADOS

Art. 21. A ETIR proverá seus serviços em 02 (dois) grupos de atuação, reativos e proativos, sendo sua atuação principal os serviços proativos.

Tabela 1 – Descrição dos Serviços Proativos prestados pela ETIR

Serviços Proativos	
Serviço	**Descrição**
Monitorar Incidentes	Observar os eventos de segurança com o objetivo de determinar tendências e padrões de atividades de invasores, com vistas a adotar e recomendar estratégias de prevenção adequadas. Coletar indicadores estatísticos.
Disseminar informações relativas a novos ataques e tendências	Pesquisar informações sobre novas ameaças a redes computacionais, novas soluções para conter as ameaças e informar às áreas responsáveis.
Disseminar informações de novas atualizações de *softwares*	Pesquisar informações referentes a novas atualizações dos *softwares* instalados na rede
Comunicação	Comunicar incidentes de segurança a órgão competentes para fins estatísticos.

Tabela 2 – Descrição dos Serviços Reativos prestados pela ETIR

Serviços Proativos	
Serviço	**Descrição**
Análise de incidentes	Examinar todas as informações disponíveis sobre um incidente, incluindo artefatos, evidências e *logs* relacionados ao evento.
Investigação de incidentes	Identificar o escopo do incidente, sua extensão, natureza e quais os impactos causados
Recomendação de tratamento de incidente	Após análise e investigação do incidente, a ETIR emitirá documentos com recomendações para o tratamento correto dos incidentes

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 22. A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.

Art. 23. A ETIR poderá usar as melhores práticas de Mercado, desde que não conflitem com os dispositivos presentes na Instrução Normativa GSI Nº 1, de 13 de junho de 2008, Norma Complementar nº 05/IN01/DSIC/GSIPR, Norma Complementar nº 08/IN01/DSIC/GSIPR e Norma Complementar nº 21/IN01/DSIC/GSIPR.

Art. 24. A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

Art. 25. A troca de informações e a forma de comunicação entre as ETIR, e entre estas e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

Art. 26. Os casos omissos e as situações imprevistas serão decididas pela Diretoria de Tecnologia da Informação e/ou Comitê Gestor de Segurança da Informação e Comunicações.

Art. 27. Esta Instrução Normativa entra em vigor na data de sua publicação.

À consideração superior,

Aracaju/SE, 20 de Fevereiro de 2017.

Fernando Lucas de Oliveira Farias
Diretor de Tecnologia da Informação

De acordo,

Aracaju/SE, 20 de Fevereiro de 2017.

Ailton Ribeiro de Oliveira
Presidente do Comitê Gestor de TI

ANEXO I
GLOSSÁRIO (TERMOS TÉCNICOS, SIGNIFICADOS)

CTIR GOV é o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – APF que integra o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR) e tem como finalidade o atendimento aos incidentes em redes de computadores pertencentes à APF. Além disso, atua como centro de coordenação entre as partes envolvidas, acompanhando as ações de tratamento e resposta aos incidentes de segurança.

Norma Complementar nº 05/IN01/DSIC/GSIPR de 14/Ago/09, que disciplina a criação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da APF.

Norma Complementar nº 08/IN01/DSIC/GSIPR de 19/Ago/10, que disciplina o gerenciamento de incidentes de segurança em redes de computadores realizado pelas ETIR dos órgãos e entidades da APF.

Norma Complementar nº 21/IN01/DSIC/GSIPR de 08/Out/14, que estabelece diretrizes para o registro de eventos, coleta e preservação de evidências de Incidentes de Segurança em Redes.

ETIR denominação para Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais que é o grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Plataforma GLPI é o sistema utilizado no IFS para gerenciamento da central de serviços onde o servidor realiza a abertura de **chamado** para requisição de algum serviço do **catálogo de serviços de TI**, o acesso ao sistema é realizado através do link "https://aplicacoes.ifs.edu.br/suporte", sendo o **usuário** o SIAPE e a **senha** mesma utilizada para acesso aos sistemas SIG (SIPAC, SIGRH ou SIGAA).