SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA

PORTARIA Nº 1153 DE 05 DE Agosto DE 2019

O VICE-DIRETOR EM EXERCÍCIO DA DIREÇÃO-GERAL DO CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA, no uso de suas atribuições legais conferidas pela Portaria Ministerial nº 812, publicada no D.O.U. de 24 de Junho de 2011, e de acordo com a Lei nº 6.545, de Junho de 1978, alterada pela Lei nº 8.711, de 28 de Setembro de 1993, a Lei nº 8.948, de Dezembro de 1994, a Lei nº 11.892, de 29 de Dezembro de 2008, e o Decreto nº 5.224, de 1 de Outubro de 2004,

RESOLVE:

Art. 1º Aprovar o disposto na Norma de Serviço/DTINF nº 03, de 23 de Julho de 2019, Anexo I desta portaria, que dispõe sobre instruções relativas ao Tratamento de Incidentes de Segurança da Informação no âmbito do Cefet/RJ, sob gestão e responsabilidade do Departamento de Tecnologia da Informação (DTINF).

Art. 2º Revogar a Portaria n° 1.282, de 04/10/2018.

Art. 3º Esta portaria entra em vigor na data de sua assinatura.

MAURÍCIO SALDANHA MOTTA
VICE-DIRETOR EM EXERCÍCIO DA DIREÇÃO-GERAL

Ministério de Educação
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
Departamento de Tecnologia da Informação - DTINF

ANEXO I

NORMA DE SERVIÇO/DTINF Nº 03, DE 23 DE JULHO DE 2019.

Dispõe sobre as instruções sobre Tratamento de Incidentes de Segurança da Informação no âmbito do Cefet/RJ sob gestão do Departamento de Tecnologia da Informação (DTINF) e responsabilidade da Direção Geral do CEFET/RJ.

O Departamento de Tecnologia da Informação - DTINF, no uso das suas atribuições que lhe confere a definição e orientação das políticas, estratégias, padrões técnicos e diretrizes no âmbito em Tecnologia de Informação e Comunicação (TIC), conforme descritos no Regimento Interno e Plano Diretor de Tecnologia de Informação da instituição e, considerando a necessidade de Tratamento de Incidentes de Segurança da Informação no ambiente computacional do Cefet/RJ, resolve:

Capítulo I

DAS DISPOSIÇÕES GERAIS

Art.1º Esta norma visa instruir para que os eventos de segurança da informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e ação para mitigar o impacto negativo sobre os sistemas de informação do Cefet/RJ.
Parágrafo único - A presente norma se aplica no âmbito do Cefet/RJ.

Capítulo II

DOS OBJETIVOS GERAIS

Art.2º Esta norma objetiva a implementação de ações preventivas a fim de reduzir a quantidade de incidentes de segurança da informação no âmbito institucional.

Capítulo III

DA FUNDAMENTAÇÃO NORMATIVA E LEGAL

Art 3º Esta norma foi elaborada com base na ABNT NBR-ISO/IEC-27001 [Tecnologia da Informação/Técnicas de segurança/Sistemas de Gestão de Segurança da Informação/ Requisitos] e na ABNT NBR-ISO/IEC-27002 [Tecnologia da informação/Técnicas de Segurança/Código de prática para a Gestão de Segurança da Informação].

Art 4º A presente norma está fundamentada na norma complementar 08/IN01/DSIC/GSIPR do Gabinete de Segurança Institucional Departamento de Segurança da Informação e Comunicações da Presidência da República que apresenta as diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal.

Capítulo IV

DAS DEFINIÇÕES

Art.5º Para fins desta norma, considera-se:

I - **CSIRT/DTINF**: Grupo de Resposta a Incidentes de Segurança da Informação do Departamento de Tecnologia da Informação do Cefet/RJ;

II - **CAIS**: Centro de Atendimento a Incidentes de Segurança da RNP (Rede Nacional de Ensino e Pesquisa);

III – **CERT-BR**: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet;

IV - **Endereço IP**: Protocolo de internet (*Internet Protocol*) é uma sequência numérica que identifica cada equipamento na rede;

V - **Endereço MAC**: Endereço físico associado à interface de comunicação, que conecta um dispositivo à rede;

VI - **Evento de Segurança da Informação**: é a ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da Política de Segurança da

Informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação;

VII - **CSIC**: Comissão de Segurança da Informação e da Comunicação do Cefet/RJ designada pelo Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC);

VIII - ***Log*** - é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de *log* pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

IX - ***Host***: é qualquer computador ou máquina conectado a uma rede, que conta com endereço IP e nome definidos;

X - **Vírus**: programa desenvolvido para causar danos ao usuário do computador;

XI - ***Spyware***: são programas espiões, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador;

XII - ***Malware***: é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

Capítulo V

DOS PROCEDIMENTOS

Art.6º O procedimento padronizado para o tratamento de incidentes de segurança deve compreender as seguintes etapas:

I. Recepção da denúncia ou alerta interno de atividade suspeita;
II. Medidas de contenção imediata do incidente;
III. Coleta de informações e evidências;
IV. Análise das informações e evidências;
V. Notificação dos envolvidos;
VI. Análise crítica e medidas corretivas.

Seção I
Da denúncia ou alerta interno de atividade suspeita

Art.7º As reclamações sobre o uso indevido de correio eletrônico, *spamming*, violação de direitos autorais, utilização ilícita ou qualquer atividade em desacordo com as normativas e políticas de segurança da informação, devem ser enviadas ao Setor de Segurança da

Informação (SEGUR) do Cefet/RJ pelo email segur@cefet-rj.br, com a devida comprovação da atividade relatada.

Art.8º O CSIRT/DTINF investigará e tomará ações corretivas sobre as denúncias realizadas por meio do Centro de Atendimento a Incidentes de Segurança – CAIS da RNP e do CERT-BR sobre atividade suspeita proveniente da rede do Cefet/RJ.

Parágrafo único - O SEGUR, por meio da CSIC seguirá as orientações e colaborará com as atividades do Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) em relação ao uso e divulgação de conteúdo na Internet. Para mais informações sobre o CAIS e suas políticas específicas consultar http://www.rnp.br/cais.

Art.9º O Cefet/RJ colaborará com as entidades legalmente competentes na investigação de atividades presumidamente ilícitas provenientes da rede do Cefet/RJ.

§1 - Serão investigados os alertas provenientes dos sistemas de monitoramento da rede do Cefet/RJ, iniciando o processo de tratamento de incidentes de segurança quando for observada atividade em desacordo com a Política de Segurança da Informação e Comunicação do Cefet/RJ ou com as normas pertinentes.

§2 - Serão aceitas denúncias de pessoas físicas ou entidades públicas ou privadas vítimas de atividade suspeita proveniente da rede do Cefet/RJ, quando devidamente comprovadas.

Seção II
Das Medidas de contenção imediata do incidente

Art.10 A contenção imediata do incidente se fará por meio de bloqueio de acesso do *host* envolvido no incidente da rede do Cefet/RJ, sendo mantido até a solução do problema ou término da investigação.

Seção III
Das Coletas de informações e evidências

Art.11 As informações e evidências sobre as atividades denunciadas serão coletadas por meio dos *logs* dos diversos sistemas e serviços disponíveis na rede do Cefet/RJ.

Seção IV
Das Análises das informações e evidências

Art.12 Todas as informações e evidências serão analisadas para investigar o *host* que gerou o incidente denunciado.

§1 - A identificação do *host* compreenderá a determinação do seu endereço IP e endereço MAC da interface de rede, nome, *switch* e porta de acesso, bem como prédio, departamento, sala e usuário, se possível.

§2 - O tipo de atividade será determinado pelas informações evidenciadas em *logs* de serviços.

§3 - As evidências necessárias serão compiladas para a formalização da notificação dos envolvidos.

Seção V
Da Notificação dos envolvidos

Art.13 Será encaminhada notificação por escrito da atividade denunciada ou sob investigação à área onde se situa o *host* envolvido.

Art.14 Cabe ao responsável pelos usuários da máquina que seja alvo de investigação, a determinação da origem da atividade, com sua adequada comprovação.

Art. 15 Como origem pode-se considerar:

I. Atividade realizada pelo usuário;
II. Atividade realizada por terceiro com autorização do usuário;
III. Atividade realizada por invasor, sem autorização ou conhecimento do usuário.

Art.16 Como evidência da origem da atividade pode-se considerar:

I. *Logs* de acesso local ou remoto da máquina;
II. *Logs* de detecção de vírus, *spyware, malware*, etc.;
III. Outras informações que possam identificar claramente a origem da atividade.

Art.17 O responsável pela área do incidente deverá responder a notificação por escrito, com a comprovação da origem da atividade e as medidas administrativas tomadas para evitar reincidência do usuário.

Seção VI
Das Análise crítica e medidas corretivas

Art.18 A CSIC avaliará a resposta do responsável pela área e determinará as medidas corretivas no *host* identificado.

§1 - Nos casos comprovados de invasão, o *host* permanecerá bloqueado até a implantação das medidas corretivas apresentadas.

§2 - Nos casos de atividades maliciosas de usuário, o *host* permanecerá bloqueado por 30 dias, sem prejuízo das medidas administrativas tomadas pelo centro responsável.

§3 - Em caso de reincidência de atividade mal-intencionada no host identificado, o mesmo permanecerá bloqueado por 90 dias, sem prejuízo do processo de tratamento de incidentes definido neste documento.

Art.19 Se ocorrer nova reincidência após o bloqueio de 90 dias, o *host* perderá definitivamente o acesso direto à rede do Cefet/RJ.

Capítulo IV
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art.20 Os casos omissos nesta norma serão levados em consideração pela chefia do Departamento de Tecnologia da Informação em conjunto com a Comissão de Segurança da Informação e Comunicação (CSIC) e Comitê Gestor de TI (COGTI), devendo prestar contas a esta diretoria e ao Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC).

Art.21 Esta norma entra em vigor na data de sua publicação.

Julliany Sales Brandão
Chefe do Departamento de Tecnologia da Informação - DTINF
Mat. SIAPE nº 1634929