Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Minas Gerais
Reitoria

Publicado em
22/10/2014

INSTITUTO FEDERAL
MINAS GERAIS
Reitoria

Boletim de Serviço

Lei nº 4965 de 05/05/1966

Outubro/2014 • Extraordinário - Nº 04

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Minas Gerais
Reitoria

INSTITUTO FEDERAL
MINAS GERAIS
Reitoria

Boletim de Serviço

Lei nº 4965 de 05/05/1966

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS
GABINETE DO REITOR
Avenida Professor Mário Werneck, nº. 2590, Bairro Buritis, Belo Horizonte, CEP 30575-180, Estado de Minas Gerais

PRESIDENTE DA REPÚBLICA
Dilma Vana Rousseff

MINISTRO DA EDUCAÇÃO
José Henrique Paim

SECRETÁRIO DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
Aléssio Trindade de Barros

REITOR DO INSTITUTO FEDERAL MINAS GERAIS
Caio Mário Bueno Silva

CHEFE DE GABINETE
Marilícia Brandão Mól Gonçalves

PRÓ-REITOR DE PLANEJAMENTO E ORÇAMENTO
Rainer de Paula

PRÓ-REITOR DE ADMINISTRAÇÃO
Edmar Geraldo de Oliveira

PRÓ-REITOR DE ENSINO
Washington Santos da Silva

PRÓ-REITORA DE PESQUISA, INOVAÇÃO E PÓS-GRADUAÇÃO
Lydia Armond Muzzi

PRÓ-REITOR DE EXTENSÃO
Lucas Carlúcio Magalhães

DIRETOR DE TECNOLOGIA DA INFORMAÇÃO
Renato Machado de Godoy

DIRETOR DE ARTICULAÇÃO E POLÍTICAS ESPECIAIS
Josiler Magno Macedo Reis

DIRETOR DE ORÇAMENTO
Roberto de Oliveira Bezerra

DIRETORA DE GESTÃO DE PESSOAS
Cláudia Maria Teixeira Alves

Portarias

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS
GABINETE DO REITOR
Avenida Professor Mário Werneck, nº. 2590, Bairro Buritis, Belo Horizonte, CEP 30575-180, Estado de Minas Gerais

PORTARIA Nº.1524 DE 22 DE OUTUBRO DE 2014.

Dispõe sobre a aprovação do Regimento Interno da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais.

O **REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS**, no uso das atribuições que lhe são conferidas pelo Estatuto da Instituição, republicado com alterações no Diário Oficial da União do dia 28 de junho de 2012, Seção 1, Págs. 130, 131 e 132 e pelo Decreto de 12 de agosto de 2011, publicado in DOU de 15 de agosto de 2011, Seção 2,

RESOLVE:

Art. 1º APROVAR o Regimento Interno da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais, na forma do regulamento anexo.

Art. 2º. Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviços deste Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais.

Belo Horizonte, Estado de Minas Gerais, 22 de outubro de 2014.

Professor **CAIO MÁRIO BUENO SILVA**
Reitor do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais

REGIMENTO INTERNO DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS (ANEXO À PORTARIA 1524/2014)

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Incidente de Segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

CSI: Comitê de Segurança da Informação.

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 dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

POSIC: Política de Segurança da Informação e Comunicações.

Risco: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

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.

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

Incidente: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

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.

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 Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI.

Ativos de Informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

CAPÍTULO II
DA MISSÃO

Art. 1º - A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais Central (ETIRC) do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais, assim como as equipes locais nos *campi*, têm como missão:

I - facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais no âmbito de seu público-alvo;

II - promover a recuperação de sistemas;

III - receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, assim como a qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IV - informar as violações da POSIC ao Gestor de Segurança da Informação para que sejam submetidas ao CSI (Comitê de Segurança da Informação) e apuradas por este, a fim de contribuir para a adequada prestação dos serviços do IFMG;

Parágrafo único: O descumprimento ou a violação de um ou mais itens da POSIC deverão ser analisados pelo CSI (Comitê de Segurança da Informação) e deliberados, a fim de instaurar sindicância.

CAPÍTULO III
DO PÚBLICO ALVO

Art. 2º - O público-alvo da ETIRC é formado por todos os usuários dos serviços de Tecnologia da Informação na Reitoria do IFMG.

Art. 3º - O público-alvo das ETIR's locais é formado por todos os usuários dos serviços de Tecnologia da Informação nos *campi* do IFMG.

Art. 4º - As ETIR's locais deverão enviar relatório mensal ao Gestor de Segurança da Informação sobre eventos e incidentes de segurança da informação ocorridos em sua área de atuação, com vistas a permitir que sejam dadas soluções integradas para o IFMG, bem como a geração de estatísticas.

Art. 5º - Por meio do Gestor de Segurança da Informação, a ETIRC comunicará a ocorrência de incidentes de segurança em redes de computadores ao Centro de Tratamento e Resposta de Incidentes em Redes Computacionais – CTIR GOV, conforme procedimentos definidos pelo próprio CTIR GOV, para permitir que haja

soluções integradas para a Administração Pública Federal, bem como a geração de estatísticas.

Parágrafo único: A ETIRC, assim como as ETIR's locais, deverão se reportar ao Gestor de Segurança da Informação. Além disso, as equipes devem manter relacionamento entre si para aperfeiçoamento técnico e para o trato de informações referentes aos incidentes de segurança em redes computacionais ocorridos no IFMG.

CAPÍTULO IV
DO MODELO DE IMPLEMENTAÇÃO

Art. 6º - O modelo utilizado pelas ETIR's será misto e composto pela ETIR Central (ETIRC) e equipes distribuídas por unidades, campus e conveniada (ETIR's).

Art. 7º - A ETIRC será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as equipes descentralizadas, além de ser a responsável, perante toda a organização, pela comunicação com o Centro de Tratamento e Resposta de Incidentes em Redes Computacionais CTIR GOV.

Art. 8º - As ETIR's serão responsáveis por implementar as estratégias e exercer as atividades na unidade, campus ou conveniada que configure como seu público-alvo.

CAPÍTULO V
DA ESTRUTURA ORGANIZACIONAL

Seção I
Da Posição da ETIR

Art. 9º - A ETIRC, assim como as ETIR's locais, ficarão subordinadas ao Comitê Gestor de Segurança da Informação na estrutura organizacional do IFMG.

Seção II
Do Agente Responsável

Art. 10º - São atribuições do Agente Responsável pela ETIRC e pelas ETIR's locais:

I - Coordenar a instituição, a implementação e a capacitação das equipes, bem como a manutenção da infraestrutura necessária;

II - Criar os procedimentos internos;

III - Gerenciar as atividades desempenhadas pelas equipes;

VI - Distribuir tarefas para as equipes;

V - Manter a comunicação com o Centro de Tratamento e Resposta de Incidentes em Redes Computacionais – CTIR Gov perante todo o IFMG.

Parágrafo Único: Competem ao Gestor de Segurança da Informação as atribuições do Agente Responsável e a coordenação das Equipes de Tratamento de Incidentes em Redes Computacionais do IFMG.

Seção III
Das Equipes

Art. 11º - É de competência das equipes:

I - Receber, analisar, classificar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes de computadores, além de armazenar registros para formação de séries históricas como subsidio estatístico;

II - Recolher provas logo após a ocorrência de um incidente de Segurança da Informação e Comunicações;

III - Executar análises críticas sobre os registros de falhas para assegurar que estas foram satisfatoriamente resolvidas;

IV - Investigar as causas dos incidentes de Segurança da Informação e Comunicações;

V - Implementar mecanismos, de maneira uniforme, para permitir a quantificação e o monitoramento dos tipos, volumes e custos de incidentes, além das falhas de funcionamento;

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

VII - As equipes deverão manter diálogo entre si, por meio de lista de discussão, compartilhando informações e lições aprendidas a respeito dos riscos e vulnerabilidades encontradas em seus respectivos *campi* (assim como quaisquer informações a respeito de incidentes ocorridos ou em potencial), a fim de que sejam sanados de forma integrada;

VIII - Promover treinamentos sobre segurança da informação e comunicações a todos os usuários que utilizam as informações de propriedade ou sob guarda do IFMG, ou que utilizem serviços de tecnologia da informação do IFMG, respeitado seu público-alvo e em concordância com as definições da ETIRC;

IX - Garantir que os incidentes em Redes Computacionais ocorridos no IFMG sejam monitorados e reportados ao ETIRC tão breve sejam identificados;

X - As equipes poderão realizar - mediante solicitação formal de outra equipe local e mediante autorização da ETIRC - testes de identificação de vulnerabilidades nos ativos de informação referentes a seu público-alvo ou em casos externos a ele. Os testes deverão ser programados e documentados em relatório contendo metodologia utilizada, resultados e estratégia para correção. O relatório deverá ser enviado em até 10 (dez) dias úteis para a ETIR solicitante com cópia para a ETIRC. Os procedimentos deverão seguir as orientações devidamente normatizadas a serem expedidas pela ETIRC;

XI - É de responsabilidade da ETIRC e das equipes locais a criação de políticas de uso aceitável de recursos de TI e dos ativos de informação relacionados ao seu público-alvo. Tais políticas deverão ser encaminhadas ao CSI (Comitê de Segurança da Informação) por meio do Gestor de Segurança da Informação, a fim de que sejam avaliadas e aprovadas para uso e ampla divulgação.

§ 1º É de responsabilidade da ETIRC manter diálogo com outras Equipes de Tratamento de Incidentes em Redes de Computadores externas ao IFMG, com o intuito

exclusivo de simples cooperação. Os contatos deverão ser mantidos apenas para orientação e auxílio na resposta a incidentes.

§ 2º As equipes deverão guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro e Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov.

§ 3º Os testes de identificação de vulnerabilidades não fazem parte do catálogo de serviços das equipes.

Art. 12º - A ETIRC será composta por:
I - Gestor de Segurança da Informação;
II – Diretor de TI
II – Um Analista de TI;

Art. 13º - Caso necessário, poderão ser convocados para comporem extraordinariamente a ETIRC:
I – Um dos Auditores em exercício no IFMG
II - Quaisquer membros do Comitê de Segurança da Informação.

Art. 14º - Para cada uma das posições poderá ser designado 1 (um) suplente, com conhecimento técnico e condições de substituir o titular na execução de todas as suas atribuições.

Art. 15º - As ETIR's locais serão compostas por:
I - Coordenador de TI local;
II - Técnico de TI.

§ 1º Compete ao Coordenador de TI local responder pelas atividades da ETIR da qual é membro, devendo comunicar, de imediato, ao Gestor de Segurança da Informação do IFMG, a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação, conforme orientações da ETIRC.

§ 2º Em unidades em que houver apenas um membro no departamento de TI, este constituirá a ETIR Local sob supervisão da ETIRC.

§ 3º Em unidades em que não houver equipe de TI, as atividades serão realizadas pelos membros da ETIRC ou por membros designados por ela.

CAPÍTULO V
DA AUTONOMIA

Art. 16º - A autonomia das ETIR's locais será compartilhada. As equipes trabalharão em conjunto com os outros setores da organização, a fim de participar do processo de tomada de decisão.

CAPÍTULO VI
DO CÓDIGO DE CONDUTA

Art. 17º - Os membros participantes das equipes, ao atuarem em atividades de tratamento de incidentes de segurança da informação, deverão se orientar pelo código de conduta a seguir.

I - Manter a confidencialidade de informações referentes às vítimas e aos envolvidos, assim como qualquer informação que possa prejudicar as atividades de identificação de causas e efeitos, investigação e resposta. Poderão ocorrer exceções quando houver necessidade e para garantir o bom desempenho das atividades, mediante grave ameaça ao direito à vida ou entre os membros das equipes.

II - Atuar com cordialidade, urbanidade, disponibilidade e respeito no trato com vítimas, envolvido e demais membros, respeitando suas limitações e capacidades individuais.

III - Responder com prontidão às solicitações e aos informes de incidentes de segurança e vulnerabilidades encontrados.

IV – Atuar com honestidade, veracidade, sinceridade e lealdade.

V – Buscar constantemente boa reputação.

VI – Não utilizar nenhum dos conhecimentos adquiridos durante as atividades para causar danos a terceiros e ao IFMG.

VII – Agir com discrição e moderação ao responder incidentes - com ênfase nas mídias internas e externas -, respeitando hierarquicamente o Comitê de Segurança da Informação como o responsável pela divulgação.

VIII – Respeitar a hierarquia das equipes, tanto interna quanto externamente ao seu público-alvo.

CAPÍTULO VII
DOS SERVIÇOS

Art. 14º - O catálogo de serviços das equipes será composto dos seguintes itens:

I - TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS

I.I - Definição: consiste em receber, filtrar, classificar e responder às solicitações e alertas; além de realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

I.II - Descrição das funções e procedimentos que compõem o serviço: Os membros das equipes realizarão as atividades e procedimentos de acordo com diretrizes devidamente normatizadas a serem expedidas pela ETIRC;

I.III - Disponibilidade do serviço: Será executado quando houver detecção de um incidente pela sua respectiva unidade através da ETIR local;

I.IV - Metodologia para execução do serviço: Os membros das equipes locais analisarão os relatórios gerados pelos aplicativos devidamente instituídos no IFMG. As decisões serão tomadas a partir das informações obtidas. As dúvidas a respeito dos incidentes deverão ser tratadas em conjunto com as demais equipes, conforme inciso VII do Art. 11 deste documento.

II - DISSEMINAÇÃO DE INFORMAÇÕES RELACIONADAS À SEGURANÇA

II.I - Definição: Este serviço fornece, de maneira abrangente, o acesso às informações relacionadas à Segurança da Informação e Comunicações aos usuários que utilizam as informações de propriedade (ou sob guarda do IFMG) ou os serviços de tecnologia da informação do IFMG;

II.II - Descrição das funções e procedimentos que compõem o serviço: As equipes locais realizarão eventos e reuniões com o objetivo de divulgar a POSIC e as políticas do governo federal referentes à segurança da informação;

II.III - Disponibilidade do serviço: Será executado quando a ETIR local detectar a necessidade deste evento, por meio de atualizações da legislação ou mediante solicitação da ETIRC (de acordo com o cronograma anual de atividades de TI).

II.IV - Metodologia para execução do serviço:

a) O Coordenador de TI local deverá se reunir com o público-alvo para expor as informações;

b) O Gestor de Segurança da Informação deverá se reunir com o público-alvo localizado na Reitoria para expor as informações.

CAPÍTULO VIII
DAS REFERENCIAS NORMATIVAS

I - Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

II - Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

Arte: Secretaria de Comunicação e Eventos / Reitoria

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS

Avenida Professor Mário Werneck, nº. 2590, Bairro Buritis, Belo Horizonte, CEP 30575-180, Estado de Minas Gerais
www.ifmg.edu.br