TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

PORTARIA Nº 185/2018

Institui a Equipe de Tratamento e Resposta a incidentes em Redes e Ambientes Computacionais – ETIR – e dá outras providências.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS, no uso de suas atribuições legais e regimentais e considerando o disposto no art. 26 da Resolução TSE nº 23.501, de 19 de dezembro de 2016, que "Institui a Política de Segurança da Informação – PSI – no âmbito da Justiça Eleitoral",

RESOLVE:

Art. 1º Fica instituída a Equipe de Tratamento e Resposta a Incidentes em Redes e Ambientes Computacionais – ETIR –, com a finalidade de receber, analisar, classificar e tratar notificações e atividades relacionadas a incidentes de segurança em ambientes de computadores, responder às notificações e armazenar registros para a formação de séries históricas, como subsídio estatístico e para fins de auditoria.

Art. 2º Para os efeitos desta portaria e das atribuições da ETIR, considera-se:

I – artefato malicioso: 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;

II – 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;

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

IV – tratamento de incidentes de segurança em redes e ambientes computacionais: serviço que consiste em receber, filtrar e classificar solicitações e alertas, responder a eles e realizar análises dos incidentes de segurança, extraindo informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

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

Art. 3º Compete à ETIR:

I – coordenar as atividades de tratamento e resposta a incidentes em redes e ambientes computacionais;

II – assessorar a Comissão de Segurança da Informação – CSI – na avaliação e na análise de assuntos relativos ao tratamento de incidentes de segurança da informação, bem como coordenar as ações de resposta a esses incidentes, no âmbito da Secretaria de Tecnologia da Informação;

III – propor ao Gestor da Segurança da Informação a regulamentação de matérias afetas ao tratamento de incidentes de segurança da informação do Tribunal;

IV – acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes ao tratamento de incidentes de segurança da informação;

V – colaborar, quando solicitado, na realização de auditorias no âmbito do Tribunal, no intuito de aferir o nível de qualidade das ações de resposta a incidentes;

VI – definir os procedimentos a serem executados ou as medidas de recuperação a serem adotadas durante um ataque e participar de discussões com as demais unidades do Tribunal sobre ações a serem tomadas ou possíveis repercussões, se os procedimentos não forem seguidos;

VII – acompanhar o cenário mundial no contexto de segurança da informação e aplicar esse conhecimento na análise das vulnerabilidades e correções necessárias do nosso ambiente;

VIII – comunicar ao Gestor de Segurança da Informação, em até 72 horas, os incidentes de segurança ocorridos.

Art. 4º Integram a ETIR servidores da Secretaria de Tecnologia da Informação – STI, sob a responsabilidade do Núcleo de Segurança da Informação – NSINF –, e os titulares das seguintes áreas da STI:

I – Núcleo de Segurança da Informação;

II – Seção de Gerência de Infraestrutura e Redes;

III – Seção de Administração de Banco de Dados;

IV – Seção de Monitoramento e Segurança dos Ambientes Computacionais de Produção;

V – Seção de Desenvolvimento de Sistemas;

VI – Seção de Suporte Operacional.

§ 1º Os integrantes da ETIR não estão sujeitos a dedicação exclusiva, atuando mediante convocação, quando da necessidade de solução de incidentes de segurança.

§ 2º Os titulares das áreas especificadas nos incisos deste artigo poderão ter suplentes formalmente designados.

Art. 5º A ETIR atuará em consonância com as unidades do Tribunal no tocante ao processo de tomada de decisão sobre as medidas a serem adotadas quanto à prevenção e à solução dos incidentes de segurança.

Parágrafo único. Em relação exclusivamente ao contexto de TI, a ETIR, sempre que possível, deverá:

I – preservar as evidências digitais do incidente;

II – executar imediatamente as medidas de recuperação, com a finalidade de restabelecer rapidamente a continuidade dos serviços eventualmente interrompidos;

III – recomendar ao Gestor de Segurança da Informação os procedimentos preventivos necessários para evitar novos incidentes;

IV – atuar imediatamente, de forma reativa e preventiva, sempre que identificar incidente ou risco iminente que possa causar danos à rede, aos usuários ou às informações corporativas do Tribunal;

V – relatar ao Gestor de Segurança da Informação os incidentes de segurança ocorridos e as soluções adotadas, a fim de permitir a geração de estatísticas e soluções integradas.

Art. 6º São usuários dos serviços da ETIR os Magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e os cidadãos atendidos diretamente ou por meio dos sistemas disponíveis no portal do TRE-MG na internet.

§ 1º Os usuários internos registrarão as ocorrências que possam ser qualificadas como incidentes de segurança por meio de abertura de chamado no Sistema de Solicitação de Serviços – SOS – ou por meio do Processo Administrativo Digital – PAD.

§ 2º As notificações dos usuários externos relativas à segurança da informação deverão ser encaminhadas ao Gestor de Segurança da Informação.

Art. 7º Esta portaria entra em vigor na data de sua publicação.

Des. **PEDRO BERNARDES**
Presidente

Informações de Chancela Digital

As páginas anteriores a esta correspondem ao documento eletrônico nº 192441/2018, registrado no sistema PAD (Processo Administrativo Digital) do Tribunal Regional Eleitoral de Minas Gerais.

Este documento eletrônico foi assinado por:

	PEDRO BERNARDES DE OLIVEIRA *Assinado eletronicamente em 20/08/2018 18:09:57* *Lei 11.419/2006, art. 1º, § 2º, IIIb*

O documento eletrônico original pode ser obtido junto ao Tribunal Regional Eleitoral de Minas Gerais.