Tribunal Regional Eleitoral - RJ
Diretoria Geral
Secretaria de Administração
Coordenadoria de Gestão Documental, Informação e Memória

RESOLUÇÃO TRE-RJ Nº 1272, DE 14 DE MARÇO DE 2023.

Reestrutura e regulamenta o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) do Tribunal Regional Eleitoral do Rio de Janeiro.

O TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a **Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça (https://atos.cnj.jus.br/atos/detalhar/3706)**, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a **Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça (https://atos.cnj.jus.br/atos/detalhar/3975)**, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), e a **Portaria CNJ n.º 162, de 10 de junho de 2021 (https://atos.cnj.jus.br/atos/detalhar/3982)**, que estabeleceu, em seu **Anexo I (https://atos.cnj.jus.br/atos/detalhar/3982)**, padrões de funcionamento e competência de atuação das Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO a **Resolução n.º 23644, de 1º de julho de 2021, do Tribunal Superior Eleitoral (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO o disposto nos **Acórdãos nºs 866/2011 (https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/NUMACORDAO%253A866%2520ANOACORDAO%253A2011/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520d 594/2011 (https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/NUMACORDAO%253A594%2520ANOACORDAO%253A2011/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520d 7312/2010 (https://pesquisa.apps.tcu.gov.br/#/resultado/acordao-completo/*/NUMACORDAO%253A7312%2520ANOACORDAO%253A2010/%2520)** e **2746/2010 (https://pesquisa.apps.tcu.gov.br/#/resultado/acordao-completo/*/NUMACORDAO%253A2746%2520ANOACORDAO%253A2010/%2520)** - Plenário, do Tribunal de Contas da União, que determinam a instituição de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais; e

CONSIDERANDO, ainda, o teor do Processo SEI n.º 2022.0.000035125-4,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º A estrutura e o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) do Tribunal Regional Eleitoral do Rio de Janeiro obedecerão ao disposto nesta Resolução.

Art. 2º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética tem por missão planejar, coordenar e executar as atividades de tratamento e resposta a incidentes de segurança da informação, buscando preservar os dados, informações, softwares, dispositivos móveis e dispositivos da infraestrutura do Tribunal Regional Eleitoral do Rio de Janeiro, além de armazenar registros para formação de séries históricas, como subsídio estatístico, e para fins forenses e de auditoria.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos desta Resolução e de suas regulamentações, aplicam-se as seguintes definições:

I - EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA (ETIR): grupo de pessoas com a responsabilidade de receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança da informação, tradicionalmente denominado Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - EVENTO - qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação e comunicação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

III - INCIDENTE DE SEGURANÇA: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

CAPÍTULO III

DO PÚBLICO-ALVO

Art. 4º A ETIR tem como público-alvo os usuários internos e externos dos ativos de informação e de processamento do Tribunal Regional Eleitoral do Rio de Janeiro.

CAPÍTULO IV

MODELO DE IMPLEMENTAÇÃO, AUTONOMIA E ESTRUTURA

Seção I

Modelo de Implementação

Art. 5º A ETIR será formada por membros das equipes de Tecnologia da Informação do próprio Tribunal que, além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança cibernética.

Art. 6º A atuação da ETIR se dará de forma predominantemente reativa, podendo o seu coordenador, excepcionalmente, atribuir responsabilidades para que seus membros exerçam atividades proativas.

Seção II

Autonomia

Art. 7º A ETIR terá autonomia compartilhada, o que significa que trabalhará em acordo com os outros setores da organização a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

§ 1º A ETIR participará no resultado das decisões, sendo, no entanto, apenas um membro no processo decisório. A Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os níveis de gestão superiores.

§ 2º Nos casos de crise cibernética, o gerenciamento da crise será conduzido pelo Comitê de Crises Cibernéticas do TRE-RJ, que direcionará as ações de tratamento e resposta, com o auxílio da ETIR, em conformidade com o Protocolo de Gestão de Crises Cibernéticas do TRE-RJ.

Art. 8º A ETIR somente poderá atuar sem aprovação dos níveis de gestão superiores nas seguintes hipóteses:

I - quando a ocorrência de um incidente exigir atuação imediata e emergencial, relacionada à segurança dos sistemas de computação ou das redes de computadores, poderá a ETIR tomar a decisão de executar medidas de mitigação como efetuar bloqueios e tornar indisponíveis os serviços afetados, submetendo, prontamente, as ações à apreciação dos níveis superiores.

II - a ETIR também poderá atuar sem esperar pela aprovação de níveis superiores de gestão nos casos em que o incidente registrado seja de simples resolução e não impacte processos de trabalho das áreas de negócio.

Seção III

Estrutura organizacional

Art. 9º A ETIR compartilhará com os níveis superiores de gestão a autonomia para desenvolver suas atividades, submetendo as medidas e ações a serem executadas para resolver os incidentes de segurança à aprovação superior, sempre que necessário, de acordo com o estipulado nos artigos 7º e 8º desta Resolução.

§ 1º A Secretaria de Tecnologia da Informação constituirá o primeiro nível de gestão superior.

§ 2º A Diretoria-Geral constituirá o segundo nível de gestão superior.

Art. 10. A ETIR terá a composição mínima de 9 (nove) membros, preferencialmente ocupantes de cargo efetivo, e será integrada necessariamente pelos seguintes servidores:

I - Secretário de Tecnologia da Informação;
II - Coordenador da Coordenadoria de Infraestrutura;
III - Coordenador da Coordenadoria de Soluções Corporativas;
IV - Coordenador de Sistemas Eleitorais;
V - Chefe do Núcleo de Defesa Cibernética.

§ 1º Os demais membros e seus substitutos serão indicados pela Secretaria de Tecnologia da Informação e nomeados pela Diretoria-Geral.

§ 2º O Secretário de Tecnologia da Informação e os servidores ocupantes de cargos de coordenadoria referidos nos incisos do caput serão substituídos em suas ausências pelos respectivos substitutos eventuais.

§ 3º A equipe será coordenada pelo Secretário de Tecnologia da Informação.

§ 4º Os membros da ETIR deverão organizar seus afastamentos de forma que permaneça um contingente mínimo para desempenho de suas atividades regulares.

CAPÍTULO V

DAS ATRIBUIÇÕES

Art. 11. São atribuições da Equipe de Tratamento e Resposta a Incidentes de Segurança

Cibernética:

I - receber, filtrar, classificar e responder às comunicações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e identificar tendências;

II - coordenar as atividades de tratamento e resposta a incidentes de segurança da informação;

III - elaborar e manter processo de tratamento e resposta a incidentes de segurança da informação;

IV - definir e manter os procedimentos de resposta específicos (playbooks), com as ações a serem executadas e as medidas de recuperação a serem adotadas quando da ocorrência de incidentes de segurança da informação;

V - comunicar ao Gestor de Segurança da Informação do TRE-RJ a ocorrência de incidentes e informá-lo sobre o andamento do processo de tratamento e resposta;

VI - comunicar ao Comitê de Crises Cibernéticas do TRE-RJ a ocorrência de incidente crítico de segurança da informação e apoiar nas ações de tratamento e resposta inerentes a esta situação;

VII - comunicar imediatamente à unidade encarregada de dados pessoais do TRE-RJ os incidentes de segurança da informação que envolvam violação de dados pessoais;

VIII - acionar e prestar de maneira contínua informações técnicas assertivas à alta administração do Tribunal e a quem ela determinar, quando da condução, do tratamento e da resposta relacionada a incidentes críticos de segurança da informação;

IX - assessorar o Gestor de Segurança da Informação do TRE-RJ, o Diretor-Geral e o Secretário de Tecnologia da Informação na avaliação e na análise de assuntos relativos ao tratamento e resposta a incidentes de segurança da informação;

X - seguir os procedimentos para coleta e preservação de evidências e para comunicação obrigatória de eventos previstos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

XI - colaborar na realização de auditorias e análises forenses;

XII - formalizar à ETIR do Tribunal Superior Eleitoral os incidentes de segurança em redes computacionais que envolvam ou que possam vir a envolver mais de um tribunal eleitoral;

XIII - atender às orientações da ETIR do Tribunal Superior Eleitoral;

XIV - receber e acompanhar os direcionamentos da ETIR do Tribunal Superior Eleitoral e atuar em conjunto com os demais regionais nas atividades de tratamento do incidente de segurança nas redes computacionais que envolver mais de um Estado;

XV - cooperar com outras equipes de tratamento e resposta a incidentes cibernéticos ou equipes equivalentes de segurança da informação de acordo com os protocolos de cooperação estabelecidos pelo Poder Judiciário;

XVI - solicitar apoio multidisciplinar para responder aos incidentes de segurança de maneira adequada e tempestiva, em áreas como:

a) tecnologia da informação;
b) segurança da informação;
c) jurídica, pesquisas judiciárias;
d) comunicação;
e) controle interno;
f) segurança institucional, entre outras;

XVII - interagir com:

a) a ETIR do Tribunal Superior Eleitoral;
b) as ETIRs dos demais tribunais regionais eleitorais;
c) o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);
d) o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo concernente a assuntos de segurança cibernética - CTIR Gov;
e) outras equipes de tratamento e resposta a incidentes cibernéticos ou equipes equivalentes de segurança da informação de acordo com os protocolos de cooperação estabelecidos pelo Poder Judiciário, bem como outras entidades públicas e fornecedores de software, hardware e serviços, quando necessário ao tratamento de incidentes de segurança cibernética;

XVIII - elaborar e manter relação de contatos de entes externos para auxílio e comunicação.

CAPÍTULO VI

DA COMUNICAÇÃO DE INCIDENTES

Art. 12. Todos os usuários internos e externos dos ativos de informação e de processamento do Tribunal Regional Eleitoral do Rio de Janeiro devem obrigatoriamente comunicar supostos incidentes de segurança da informação.

Art. 13. A comunicação de incidentes deverá ser feita à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR, por e-mail.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 14. As unidades vinculadas à Secretaria de Tecnologia da Informação e as unidades organizacionais envolvidas pelo incidente deverão priorizar o atendimento à ETIR quando instadas a participar no processo de tratamento e resposta a incidentes de segurança cibernética.

Parágrafo único. As atividades da ETIR terão prioridade sobre aquelas designadas pelos chefes imediatos de seus respectivos integrantes.

Art. 15. A revisão desta Resolução será realizada pela Comissão de Segurança da Informação em intervalos não superiores a 2 (dois) anos ou sempre que se fizer necessário ou conveniente para este Tribunal.

Art. 16. Fica revogada a **Resolução TRE-RJ nº 1066/2018 (https://www.tre-rj.jus.br/legislacao/compilada/resolucoes/2018/resolucao-tre-rj-no-1066-de-29-de-agosto-de-2018)**.

Art. 17. Esta Resolução entrará em vigor na data de sua publicação.

Rio de Janeiro, 14 de março de 2023.

Desembargador ELTON MARTINEZ CARVALHO LEME

Presidente do Tribunal Regional Eleitoral do Rio de Janeiro

Este texto não substitui o publicado no **DJE TRE-RJ nº 70, de 17/03/2023, p. 223 (https://dje.tse.jus.br/dje/pdf/v1/edicao/102727#page=223)**