PORTARIA Nº 1820/2022
Institui Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

A PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, no uso de suas atribuições,

CONSIDERANDO os termos da Resolução do Conselho Nacional de Justiça (CNJ) n° 370, de 28 de janeiro de 2021, que estabelece a nova Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e as diretrizes para sua governança, gestão e infraestrutura;

CONSIDERANDO os termos da Resolução CNJ n° 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO os termos da Portaria CNJ n° 162, de 10 de junho de 2021, que aprova protocolos e manuais criados pela Resolução CNJ n° 396/2021; e

CONSIDERANDO o que dispõe a Resolução do Órgão Especial n° 07, de 24 de fevereiro de 2022, que dispõe sobre a criação do Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC) no âmbito do Poder Judiciário do Estado do Ceará e dá outras providências.

RESOLVE:

Art. 1° Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, no âmbito do Poder Judiciário Estadual cearense.

Parágrafo único: A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR tem como missão 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, relacionados às redes de computadores, preservando os dados, as informações e a infraestrutura do Poder Judiciário do Estado do Ceará.

Art. 2° Para os efeitos desta portaria consideram-se:

I – **equipe de tratamento e resposta a incidentes de segurança de cibernética (ETIR)**: Denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia;

II – **agente responsável pela ETIR**: servidor público do Poder Judiciário incumbido de chefiar e gerenciar a ETIR;

III – **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;

IV – **comunidade ou público-alvo:** conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR;

V – **centro de prevenção, tratamento e resposta a incidentes cibernéticos do Poder Judiciário (CPTRIC-PJ)**: órgão nacional coordenado pelo Conselho de Nacional de Justiça que funcionará como canal oficial de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos;

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

VII – **serviço:** conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da ETIR;

VIII – **tratamento de incidentes de Segurança em Redes Computacionais:** 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;

IX – **vulnerabilidade:** conjunto de fatores internos ou causa potencial de um incidente indesejado que pode resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

X – **usuário:** qualquer indivíduo ou organização que utiliza ou trabalha com algum sistema, dispositivo ou serviço de TIC oferecido pelo TJCE; e

XI – **registros:** informações sobre a quantidade e o tipo dos alertas e incidentes de segurança da informação.

Art. 3° Compete a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR:

I – receber, analisar e classificar os logs de segurança para identificar os incidentes de segurança da informação;

II – coordenar as atividades de tratamento e respostas a incidentes de segurança da informação;

III – definir o plano de resposta a incidentes, com os procedimentos a serem executados e as medidas de recuperação a serem adotadas quando da ocorrência de incidentes de segurança da informação;

IV – comunicar ao Comitê de Governança de Segurança da Informação e Gestão de Crises (CGSICC) do TJCE a ocorrência de incidente crítico de segurança da informação e apoiar nas ações de tratamento e resposta inerentes a esta situação;

V – 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;

VI – colaborar na realização de auditorias e análises forenses quando solicitado pelo Secretário de Tecnologia da Informação do TJCE;

VII – comunicar à unidade encarregada de dados pessoais do TJCE os incidentes de segurança da informação, relacionados a dados pessoais;

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

IX – 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; e

XII – interagir com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).

Art. 4° A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação atuará em consonância com as práticas, os processos e os normativos internos do Tribunal no tocante ao processo de tomada de decisão sobre as medidas a serem adotadas quanto à prevenção, ao tratamento e às respostas a incidentes de segurança da informação.

Parágrafo único. Em relação exclusivamente ao contexto de TIC, a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, sempre que possível, deverá:

I – preservar as evidências digitais do incidente;

II – coordenar as medidas de recuperação, com a finalidade de restabelecer a continuidade dos serviços interrompidos;

III – recomendar ao Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC) do TJCE os procedimentos preventivos necessários para evitar novos incidentes;

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

V – relatar ao Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC) do TJCE e ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) os incidentes críticos de segurança da informação ocorridos e as soluções adotadas, a fim de permitir a geração de estatísticas e soluções integradas.

Art. 5° Com exceção dos incidentes críticos, a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação possui plena autonomia para realizar ações necessárias na recuperação de incidentes de segurança e poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão, comunicando imediatamente as providências adotadas ao Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC).

Art. 6° Nos casos de incidentes críticos, a responsabilidade pelo direcionamento e pela condução das ações de tratamento e resposta será do Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC).

Art. 7° Integram a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR:
I - Supervisor(a) Operacional do Serviço de Segurança da Informação, que será o agente responsável pela ETIR;
II - Gerente da Gerência de Infraestrutura de TI, que substituirá o agente responsável pela ETIR quando necessário;
III - Coordenador(a) da Coordenadoria de Suporte Técnico;
IV - Coordenador(a) da Coordenadoria de Gestão de Serviço;
V - Gerente da Gerência de Sistemas;
VI -Coordenador(a) da Coordenadoria de Desenvolvimento de Sistemas;
VII - Coordenador(a) da Coordenadoria de Sistemas Judiciais;
VIII - Coordenador(a) da Coordenadoria de Sistemas Administrativos;
IX - Gerente da Gerência de Informática do Fórum Clóvis Beviláqua;
X - Coordenador(a) da Coordenadoria do Processo Judicial Eletrônico;
XI - Coordenador(a) da Coordenadoria de Administração de Dados; e
XII – Supervisor(a) Operacional do Serviço de Suporte e Monitoramento de Sistemas da Comarca de Fortaleza.

§ 1° Os integrantes da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação atuarão sem prejuízo de suas funções.

§ 2° A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação poderá convocar representantes de outras unidades do Tribunal de Justiça do Estado do Ceará para atuar no tratamento e resposta a incidentes de segurança da informação.

§ 3° Poderão ser convocados para auxiliar os trabalhos da ETIR prestadores de serviços com perfil de tratamento de incidentes de segurança da informação, administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede e analistas de suporte com conhecimento técnico na prevenção, detecção e tratamento de incidentes de Segurança da Informação.

Art. 8° São atribuições e responsabilidades de cada membro da ETIR:

I – Agente responsável pela ETIR:
a) prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe;
b) prover infraestrutura necessária para o funcionamento da ETIR;
c) garantir que os incidentes em Redes Computacionais do TJCE sejam registrados e investigados;
d) assegurar que haja canal de comunicação com os usuários informantes de incidentes de segurança da informação;
e) interagir com as demais áreas do TJCE durante os incidentes;
f) prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados a segurança da informação e comunicação;
g) planejar, coordenar e orientar as atividades relacionadas à gestão de incidentes;
h) informar às autoridades competentes os assuntos relacionados a incidentes de redes computacionais; e
i) exercer funções necessárias para implementação e manutenção das atividades da ETIR.

II – Gerente da Gerência de Infraestrutura de TI, Coordenador(a) da Coordenadoria de Suporte Técnico e Coordenador(a) da Coordenadoria de Gestão de Serviço:
a) receber notificações, prevenir, efetuar análise, investigar e conter incidentes que envolvam roteadores, switches, VOIP, tecnologias de armazenamento e processamento de informações, elementos de conectividade, estações de trabalho, banco de dados, sistemas operacionais, data center, sistemas sob sua gestão e outras soluções tecnológicas sob a vossa responsabilidade;
c) apoiar o tratamento de incidentes em sistemas; e
d) recomendar ações para tomada de decisão na recuperação do ambiente após incidentes.

III – Gerente da Gerência de Sistemas, Coordenador(a) da Coordenadoria de Desenvolvimento de Sistemas, Coordenador(a) da Coordenadoria de Sistemas Judiciais e Coordenador(a) da Coordenadoria de Sistemas Administrativos:
a) receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam Sistemas de 1° e 2° Graus, administração de dados e sistemas sob sua gestão;
b) apoiar o tratamento de incidentes em sistemas; e
c) recomendar ações para tomada de decisão na recuperação dos incidentes.

IV – Gerente da Gerência de Informática do Fórum Clóvis Beviláqua e Supervisor(a) do Serviço de Suporte e Monitoramento de Sistemas da Comarca de Fortaleza:
a) receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam Sistemas de 1° Grau;
b) apoiar o tratamento de incidentes em sistemas; e
c) recomendar ações para tomada de decisão na recuperação dos incidentes.

V – Supervisor(a) Operacional do Serviço de Segurança da Informação:
a) receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam em firewalls, antivírus, proxies, servidores, active directory, DNS, DHCP outras tecnologias de segurança informação;
c) apoiar o tratamento de incidentes em sistemas operacionais e sistemas corporativos; e
d) recomendar ações para tomada de decisões na recuperação de incidentes.

VI - Coordenador(a) da Coordenadoria do Processo Judicial Eletrônico:
a) receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam Processo Judicial Eletrônico;
b) apoiar o tratamento de incidentes em sistemas; e
c) recomendar ações para tomada de decisão na recuperação dos incidentes.

VII - Coordenador(a) da Coordenadoria de Administração de Dados:
a) receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam a administração de dados e sistemas sob sua gestão;
b) apoiar o tratamento de incidentes em sistemas; e
c) recomendar ações para tomada de decisão na recuperação dos incidentes.

Art. 9° A ETIR recomendará os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá sobre as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas. Por meio de sua gestão centralizada, trabalhará em acordo com outras unidades a fim de tomada de decisão sobre quais medidas devam ser adotadas.

Art. 10. São serviços oferecidos pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais:

I – tratamento de Incidentes de Segurança em redes computacionais: 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;

II – tratamento de artefatos maliciosos: receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou, pelo menos, sugerida, uma estratégia de detecção, remoção e defesa;

III – tratamento de vulnerabilidades: em receber informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção;

IV – emissão de alertas e advertências: em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema; e

V – criar, revisar e propor melhorias nos processos e protocolos de prevenção, detecção e tratamento de incidentes de Segurança da Informação.

Art. 11. A notificação deverá ser feita pelos seguintes canais de comunicação:

I - e-mail: etir@tjce.jus.br;

II - correspondências oficiais (memorandos, ofícios);

III - Pessoalmente, em casos emergenciais;

IV - ferramental tecnológico e eventos detectados pelo monitoramento da ETIR;

V – pelo suporte técnico:
a) chamado via CATINET; e
b) Telefone (85) 3366.2966.

Art. 12. Este ato revoga a Portaria n° 1895/2018.

Art. 13. Esta Portaria entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, aos 17 de agosto de 2022.

Desembargadora Maria Nailde Pinheiro Nogueira
Presidente do Tribunal de Justiça do Estado do Ceará

Republicada por incorreção

PORTARIA Nº 1827/2022

Dispõe sobre a designação do Juiz Substituto Arthur Moura Costa.

A Presidente do Tribunal de Justiça do Estado do Ceará, no uso de suas atribuições legais, ao apreciar o Processo Administrativo n° 8500169-43.2022.8.06.0173;

RESOLVE designar o Juiz Substituto Arthur Moura Costa, Titular da Vara Única Criminal da Comarca de Tianguá para, sem prejuízo de suas funções, responder pela 2ª Vara Cível da referida Comarca, durante licença do magistrado Felipe William Silva Gonçalves, no período de 27/08 a 03/09/2022.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, Fortaleza, 18 de agosto de 2022.

Desembargadora Maria Nailde Pinheiro Nogueira
Presidente do Tribunal de Justiça do Estado do Ceará

PORTARIA Nº 1830/2022

Dispõe sobre a designação do Juiz de Direito David Melo Teixeira Sousa.

A Presidente do Tribunal de Justiça do Estado do Ceará, no uso de suas atribuições legais, ao apreciar o Processo Administrativo n° 8500089-32.2022.8.06.0124;

RESOLVE designar o Juiz de Direito David Melo Teixeira Sousa, Titular da Vara Única da Comarca de Várzea Alegre para, sem prejuízo de suas funções, responder pela Vara Única da Comarca de Farias Brito, durante licença do magistrado Diogo Schenatto Irion, no período de 18/08 a 06/09/2022.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, Fortaleza, 18 de agosto de 2022.

Desembargadora Maria Nailde Pinheiro Nogueira
Presidente do Tribunal de Justiça do Estado do Ceará