

TRIBUNAL DE JUSTIÇA - ATOS DO PRESIDENTE

PORTARIA 02303/2026

Disponibilização: 29/09/2026 às 16h48m

PORTARIA Nº 2303/2026-GABPRESI

Institui a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) no âmbito do Poder Judiciário do Estado do Ceará.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ (TJCE), no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução do Conselho Nacional de Justiça nº 370, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o disposto na alínea "a" do inciso II do art. 21 da Resolução CNJ nº 370/2021, que prevê a necessidade de cada órgão do Poder Judiciário constituir e manter estruturas organizacionais adequadas e compatíveis ao macroprocesso de incidentes de segurança, no domínio de segurança da informação e proteção de dados;

CONSIDERANDO a Resolução do Conselho Nacional de Justiça nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ nº 162, de 10 de junho de 2021, que aprova protocolos e manuais criados pela Resolução CNJ nº 396/2021, em especial o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ) e o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ);

CONSIDERANDO a Resolução do Órgão Especial nº 03/2023, de 02 de março de 2023, que unifica o Comitê Gestor de Proteção de Dados Pessoais (CGPD) e o Comitê Gestor de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC), instituindo o Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP), ao qual compete instituir e implementar a ETIR;

CONSIDERANDO a criação da Diretoria de Segurança da Informação (DSI), vinculada à Presidência do Tribunal de Justiça, e a reestruturação administrativa da Secretaria de Tecnologia da Informação (SETIN) ocorrida no exercício de 2026, que alterou nomenclaturas, competências e vínculos hierárquicos de unidades diretamente relacionadas à gestão de incidentes de segurança da informação;

CONSIDERANDO a necessidade de adequar a composição e as atribuições da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) à nova estrutura organizacional do Tribunal, assegurando efetividade, clareza na cadeia de comando e alinhamento com as diretrizes nacionais de segurança cibernética do Poder Judiciário;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) no âmbito do Poder Judiciário do Estado do Ceará, sob a supervisão institucional da Diretoria de Segurança da Informação (DSI).

Parágrafo único. A ETIR tem como missão planejar, coordenar e executar atividades de prevenção, detecção, tratamento e resposta a incidentes de segurança da informação, preservando os dados, as informações e a infraestrutura do Poder Judiciário do Estado do Ceará, e compõe a rede de equipes vinculadas ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).

Art. 2º Para os efeitos desta Portaria, considera-se:

I — Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR): grupo multidisciplinar de resposta a incidentes de segurança da informação, composto por servidores(as) do Tribunal com atribuições técnicas e estratégicas para a prevenção, detecção, contenção, erradicação e recuperação de incidentes;

II — Coordenador(a) Estratégico(a) da ETIR: servidor(a) público do Poder Judiciário incumbido(a) da supervisão institucional da ETIR, do escalonamento de incidentes e da articulação com o Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP), a Presidência e os órgãos externos;

III — Agente Responsável pela ETIR: servidor(a) público do Poder Judiciário incumbido(a) da coordenação operacional da equipe e da gestão do ciclo de vida dos incidentes;

IV — Núcleo Estratégico e Decisório: primeira camada da ETIR, composta por gestores(as) com poder de decisão e mobilização de recursos, responsável pela coordenação estratégica e operacional da resposta a incidentes;

V — Grupo de Apoio Técnico Especializado: segunda camada da ETIR, composta por coordenadores(as) e supervisores(as) de áreas operacionais, mobilizados(as) pelo(a) Agente Responsável conforme a tipologia e a criticidade do incidente;

VI — Incidente de Segurança da Informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação, das redes de computadores, dos dados, das informações ou dos serviços de TIC do Tribunal, incluindo aqueles que envolvam dados pessoais;

VII — Incidente Crítico: incidente de segurança da informação classificado no nível mais elevado de severidade, cuja gravidade, extensão ou repercussão institucional demande a condução direta pelo CGSICCPDP, conforme critérios definidos nesta Portaria;

VIII — 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

redes de computadores;

IX — Tratamento de Incidentes: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas, realizar a análise dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;

X — 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;

XI — Comunidade ou Público-Alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas pela ETIR;

XII — Registros: informações sobre a quantidade, o tipo, a classificação e o tratamento dos alertas e incidentes de segurança da informação;

XIII — Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ): órgão técnico para assuntos de segurança da informação e cibernéticos, vinculado ao Conselho Nacional de Justiça e composto por uma Rede de Cooperação do Judiciário, conforme estabelecido pela Portaria CNJ nº 172, de 25 de maio de 2022, e pelo art. 18 da Resolução CNJ nº 396/2021.

Art. 3º Compete à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR):

I — receber, registrar, analisar e classificar os eventos e alertas de segurança para identificar incidentes de segurança da informação;

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

III — definir e manter atualizado o plano de resposta a incidentes, com os procedimentos a serem executados e as medidas de recuperação a serem adotadas;

IV — comunicar ao Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP) a ocorrência de incidentes críticos de segurança da informação e apoiar nas ações de tratamento e resposta inerentes a essa situação;

V — acionar e prestar, de maneira contínua, informações técnicas à Alta Administração do Tribunal e a quem ela determinar quando da condução, do tratamento e da resposta relacionada a incidentes críticos;

VI — colaborar na realização de auditorias e análises forenses quando solicitado pela Diretoria de Segurança da Informação, pelo CGSICCPDP ou pela Presidência;

VII — comunicar ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais do TJCE os incidentes de segurança da informação que envolvam dados pessoais, subsidiando a avaliação de risco ao(à) titular e a eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD);

VIII — acompanhar o cenário nacional e internacional no contexto de segurança da informação, aplicando esse conhecimento na análise de vulnerabilidades e na adoção de medidas preventivas e corretivas no ambiente computacional do TJCE;

IX — interagir com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);

X — preservar as evidências digitais dos incidentes;

XI — coordenar as medidas de recuperação com a finalidade de restabelecer a continuidade dos serviços interrompidos;

XII — relatar ao CGSICCPDP e ao CPTRIC-PJ os incidentes críticos ocorridos e as soluções adotadas, a fim de permitir a geração de estatísticas e soluções integradas; e

XIII — elaborar relatórios de lições aprendidas após o encerramento de incidentes relevantes, propondo melhorias nos processos, procedimentos e controles de segurança.

CAPÍTULO II

DA ATUAÇÃO, DOS PROTOCOLOS E DA AUTONOMIA

Art. 4º A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) 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.

Art. 5º A ETIR observará, em suas atividades de prevenção, detecção, tratamento e resposta a incidentes, os protocolos e manuais aprovados pela Portaria CNJ nº 162, de 10 de junho de 2021, e suas eventuais atualizações, em especial:

I — o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

II — o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ);

III — o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

Parágrafo único. O(A) Coordenador(a) Estratégico(a) da ETIR promoverá a internalização dos protocolos referidos nos incisos deste artigo, assegurando que os procedimentos operacionais da equipe estejam alinhados às diretrizes nacionais e que seus(suas) integrantes conheçam as obrigações deles decorrentes.

Art. 6º O Plano de Resposta a Incidentes de Segurança da Informação, previsto no art. 3º, inciso III, deverá ser integrado ao Plano de Continuidade de Negócio (PCN) e ao Plano de Recuperação de Desastres (PRD) do Tribunal, no que se refere aos aspectos de segurança da informação, e conterá, no mínimo:

I — procedimentos de continuidade do serviço prestado e de seu rápido restabelecimento, em conformidade com o disposto no art. 11, inciso III, da Resolução CNJ nº 396/2021;

II — procedimentos de comunicação interna, incluindo o fluxo de acionamento entre as camadas da ETIR, a comunicação com a Alta Administração, com o CGSICCPDP, com o(a) Encarregado(a) pelo Tratamento de Dados Pessoais e com as unidades operacionais do Tribunal;

III — procedimentos de comunicação externa, incluindo o reporte ao CPTRIC-PJ, a eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos(às) titulares de dados pessoais afetados(as), a comunicação a órgãos de segurança pública quando cabível e a articulação com a Assessoria de Comunicação (ASCOM) para pronunciamentos públicos.

Art. 7º Ressalvados os incidentes críticos, a ETIR possui autonomia operacional para realizar as ações necessárias à contenção e recuperação de incidentes de segurança da informação, podendo executar as medidas de resposta sem aguardar aprovação de níveis superiores de gestão, comunicando imediatamente as providências adotadas ao(à) Coordenador(a) Estratégico(a) e, por seu intermédio, ao CGSICCPDP.

Art. 8º Nos casos de incidentes críticos, a responsabilidade pelo direcionamento e pela condução das ações de tratamento e resposta será do CGSICCPDP, cabendo à ETIR a execução das medidas técnicas determinadas pelo Comitê, em conformidade com o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ).

Art. 9º Os incidentes de segurança da informação serão classificados, quanto à severidade, nos seguintes níveis:

I — Nível 1 (Baixo): incidentes com impacto limitado, que afetam poucos(as) usuários(as) ou serviços não essenciais, sem comprometimento de dados pessoais e sem repercussão institucional, passíveis de resolução pelas equipes operacionais no curso regular de suas atividades;

II — Nível 2 (Médio): incidentes com impacto moderado, que afetam um conjunto identificável de usuários(as) ou serviços de apoio, podendo envolver dados pessoais não sensíveis em quantidade restrita, e que demandam a atuação coordenada de mais de uma área técnica sob a condução do(a) Agente responsável pela ETIR;

III — Nível 3 (Alto): incidentes com impacto significativo, que afetam serviços essenciais ou um grande número de usuários(as), envolvem dados pessoais sensíveis ou grandes volumes de dados pessoais, exigem escalonamento ao(à) Coordenador(a) Estratégico(a) e comunicação ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais e ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);

IV — Nível 4 (Crítico): incidentes que se enquadrem em pelo menos um dos seguintes critérios:

a) comprometam ou ameacem comprometer a disponibilidade dos serviços essenciais de TIC do Tribunal por período igual ou superior a 2 (duas) horas;

b) envolvam vazamento, exposição ou acesso não autorizado a dados pessoais sensíveis ou a dados de grande volume de titulares;

c) envolvam comprometimento de credenciais de acesso privilegiado a sistemas críticos;

d) possam gerar repercussão institucional, midiática ou jurídica significativa;

e) envolvam ataque cibernético coordenado ou persistente contra a infraestrutura do Tribunal; ou

f) sejam assim classificados pelo(a) Coordenador(a) Estratégico(a) da ETIR, pelo CGSICCPDP ou pela

Presidência.

§1º A classificação inicial do incidente será realizada pelo(a) Agente Responsável pela ETIR com base nas informações disponíveis no momento da detecção, podendo ser reclassificada a qualquer tempo em razão da evolução do cenário.

§2º Para incidentes classificados nos Níveis 3 e 4, é obrigatória a elaboração de Relatório de Comunicação de Incidente de Segurança e de Termo de Custódia dos Ativos de Informação relacionados ao incidente, conforme modelos previstos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

§3º A Presidência do Tribunal de Justiça detalhará, em ato próprio, os critérios de classificação e os procedimentos de escalonamento e comunicação correspondentes a cada nível de severidade.

Art. 10. As ações de comunicação durante e após o tratamento de incidentes observarão os seguintes parâmetros, conforme o nível de severidade do incidente:

I — Nível 1 (Baixo): registro no sistema de gestão de incidentes e comunicação ao(à) Agente Responsável pela ETIR;

II — Nível 2 (Médio): registro do incidente no sistema de gestão de incidentes, comunicação ao(à) Agente Responsável e, quando envolver dados pessoais, comunicação ao(à) Coordenador(a) Estratégico(a) para avaliação da necessidade de acionamento do(a) Encarregado(a) pelo Tratamento de Dados Pessoais;

III — Nível 3 (Alto): registro no sistema de gestão de incidentes, comunicação imediata ao(à) Coordenador(a) Estratégico(a), acionamento do(a) Encarregado(a) pelo Tratamento de Dados Pessoais quando envolver dados pessoais, reporte ao CPTRIC-PJ e comunicação à Alta Administração;

IV — Nível 4 (Crítico): adoção de todas as providências previstas no Nível 3, acrescidas do acionamento imediato do Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP) para assunção da condução do incidente, da comunicação à Presidência e da eventual comunicação externa à Autoridade Nacional de Proteção de Dados (ANPD), aos(às) titulares afetados(as) e aos órgãos de segurança pública, conforme o caso, em articulação com a Assessoria de Comunicação Social (ASCOM).

Art. 11. No exercício das atribuições previstas nesta Portaria, o(a) Agente Responsável pela ETIR detém autonomia operacional para coordenar as ações de prevenção, detecção, contenção, erradicação e recuperação de incidentes de segurança da informação, podendo acionar, orientar e articular a atuação de todos(as) os(as) integrantes do Núcleo Estratégico e Decisório e do Grupo de Apoio Técnico Especializado, independentemente da posição hierárquica que ocupem na estrutura administrativa ordinária do Tribunal.

§1º A autonomia operacional de que trata o caput tem por finalidade assegurar a celeridade e a efetividade da resposta a incidentes, prevalecendo, durante a condução do incidente, sobre a hierarquia administrativa regular no que se refere exclusivamente às ações de tratamento e resposta.

§2º O(A) Agente Responsável pela ETIR responde funcionalmente ao(à) Coordenador(a) Estratégico(a) da ETIR, a quem reportará o andamento dos incidentes em curso e a quem caberá autorizar o escalonamento ao CGSICCPDP e à Presidência.

§3º A autonomia operacional do(a) Agente Responsável não afasta nem substitui as competências do CGSICCPDP para a condução de incidentes críticos, conforme previsto no art. 8º desta Portaria, tampouco as atribuições de supervisão institucional do(a) Coordenador(a) Estratégico(a).

§4º Na ausência ou impedimento simultâneo do(a) Agente Responsável e de seu(sua) substituto(a), a coordenação operacional da ETIR será exercida pelo(a) Coordenador(a) de Cibersegurança, aplicando-se a este(a), enquanto perdurar a substituição, a autonomia operacional prevista no caput.

§5º Os(As) integrantes da ETIR, quando acionados(as) pelo(a) Agente Responsável no contexto de um incidente em curso, devem priorizar as ações de resposta e tratamento, comunicando à sua chefia administrativa imediata, quando necessário, a natureza e a estimativa de duração do envolvimento.

CAPÍTULO III

DA COMPOSIÇÃO

SEÇÃO I

Do Núcleo Estratégico e Decisório

Art. 12. Integram o Núcleo Estratégico e Decisório da ETIR:

- I — o(a) Diretor(a) de Segurança da Informação, na qualidade de Coordenador(a) Estratégico(a) da ETIR;
- II — o(a) Diretor(a) de Infraestrutura de TI, na qualidade de Agente Responsável pela ETIR;
- III — o(a) Gerente de Cibersegurança e Ambientes Tecnológicos, na qualidade de substituto(a) do(a) agente responsável;
- IV — o(a) Coordenador(a) de Cibersegurança;
- V — o(a) Diretor(a) de Sistemas;
- VI — o(a) Diretor(a) de Tecnologia do PJe;
- VII — o(a) Diretor(a) de Inteligência Artificial e Plataformas Digitais; e
- VIII — o(a) Gerente de Informática do Fórum Clóvis Beviláqua.

§1º Os(As) integrantes do Núcleo Estratégico e Decisório atuarão na ETIR sem prejuízo de suas funções administrativas regulares.

§2º A designação dos(as) integrantes do Núcleo Estratégico e Decisório é vinculada ao cargo ou função de gestão indicado(a) nos incisos deste artigo, operando-se automaticamente a substituição na ETIR quando houver alteração do(a) titular do respectivo cargo ou função.

§3º Cada integrante do Núcleo Estratégico e Decisório terá um(a) suplente designado(a), que assumirá as

respectivas atribuições na ETIR nas ausências ou impedimentos do(a) titular, quando não houver substituto(a) formal designado(a) na estrutura administrativa ordinária do Tribunal para o cargo ou função correspondente.

§4º A indicação dos(as) suplentes será formalizada no ato de que trata o art. 28 desta Portaria.

SEÇÃO II

Do Grupo de Apoio Técnico Especializado

Art. 13. O Grupo de Apoio Técnico Especializado é composto por coordenadores(as), supervisores(as) e servidores(as) das áreas operacionais cujo conhecimento técnico é indispensável à execução das ações de resposta a incidentes de segurança da informação.

§1º A composição do Grupo de Apoio Técnico Especializado será definida por ato do(a) Coordenador(a) Estratégico(a) da ETIR, ouvidos(as) o(a) Secretário(a) de Tecnologia da Informação e o(a) Diretor(a) do Fórum Clóvis Beviláqua, e poderá ser atualizada sempre que necessário em razão de mudanças organizacionais ou operacionais.

§2º Os(As) integrantes do Grupo de Apoio Técnico Especializado serão mobilizados(as) pelo(a) Agente Responsável pela ETIR conforme a tipologia e a criticidade do incidente, dispensada a necessidade de acionamento formal individualizado a cada ocorrência.

§3º A ETIR poderá, ainda, convocar representantes de outras unidades do Tribunal para atuar no tratamento e resposta a incidentes de segurança da informação, quando a natureza do incidente assim exigir.

§4º Poderão ser convocados(as) para auxiliar os trabalhos da ETIR prestadores(as) de serviços com perfil de tratamento de incidentes de segurança da informação, administradores(as) de sistemas, de segurança, de banco de dados, de rede e analistas de suporte com conhecimento técnico na prevenção, detecção e tratamento de incidentes.

CAPÍTULO V

DAS ATRIBUIÇÕES DOS(AS) INTEGRANTES DO NÚCLEO ESTRATÉGICO E DECISÓRIO

Art. 14. São atribuições do(a) Diretor(a) de Segurança da Informação, Coordenador(a) Estratégico(a) da ETIR:

I — exercer a supervisão institucional sobre as atividades da ETIR, assegurando o alinhamento das ações de resposta a incidentes com a Política de Segurança da Informação, com as normas internas do Tribunal e com as diretrizes do Conselho Nacional de Justiça;

II — escalonar ao Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP) e à Presidência os incidentes classificados como críticos, acompanhando as deliberações do Comitê e coordenando a execução das medidas por ele determinadas;

III — representar a ETIR perante o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) e demais órgãos e entidades externos, inclusive a Autoridade Nacional de Proteção de Dados (ANPD), quando o incidente envolver dados pessoais;

IV — informar às autoridades competentes os assuntos relacionados a incidentes de segurança da informação, inclusive aqueles com potencial repercussão jurídica, institucional ou midiática;

V — articular-se com o(a) Encarregado(a) pelo Tratamento de Dados Pessoais do TJCE nos incidentes que envolvam dados pessoais, subsidiando a avaliação de risco ao(à) titular e a eventual comunicação à Autoridade Nacional de Proteção de Dados ANPD e aos(às) titulares afetados(as);

VI — prestar assessoria técnica à Alta Administração e ao CGSICCPDP na elaboração de políticas, normas e pareceres relacionados à gestão de incidentes de segurança da informação;

VII — determinar, quando necessário, a convocação de representantes de outras unidades do Tribunal ou de prestadores(as) de serviço para auxiliar nos trabalhos da ETIR;

VIII — autorizar a divulgação de alertas e comunicados de segurança dirigidos à comunidade de usuários(as) do Tribunal, em articulação com a Assessoria de Comunicação (ASCOM), quando aplicável; e

IX — prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos(as) membros(as) da ETIR.

Art. 15. São atribuições do(a) Diretor(a) de Infraestrutura de TI, Agente Responsável pela ETIR:

I — coordenar operacionalmente as atividades de tratamento e resposta a incidentes de segurança da informação, gerenciando o ciclo de vida dos incidentes desde a detecção até o encerramento;

II — garantir que os incidentes de segurança da informação sejam registrados, classificados, investigados e documentados conforme os procedimentos e protocolos definidos;

III — assegurar a existência e o funcionamento de canais de comunicação para o recebimento de notificações de incidentes por parte dos(as) usuários(as);

IV — acionar e coordenar os(as) integrantes do Núcleo Estratégico e Decisório e do Grupo de Apoio Técnico Especializado conforme a tipologia e a criticidade do incidente;

V — interagir com as demais áreas do Tribunal durante o tratamento de incidentes, conduzindo a articulação operacional entre as equipes envolvidas;

VI — planejar, orientar e supervisionar as atividades relacionadas à gestão de incidentes no nível operacional;

VII — reportar ao(à) Coordenador(a) Estratégico(a) os incidentes que demandem escalonamento, fornecendo informações técnicas tempestivas para subsidiar a tomada de decisão;

VIII — elaborar relatórios de incidentes e lições aprendidas, submetendo-os ao(à) Coordenador(a) Estratégico(a) para fins de registro, melhoria contínua e eventual encaminhamento ao CGSICCPDP e ao CPTRIC-PJ;

IX — mobilizar as coordenações e gerências subordinadas à Diretoria de Infraestrutura de TI, conforme a natureza do incidente, assegurando a disponibilidade dos recursos técnicos e humanos necessários à resposta;

e

X — exercer as demais funções necessárias à implementação e manutenção das atividades da ETIR.

Art. 16. São atribuições do(a) Gerente de Cibersegurança e Ambientes Tecnológicos, substituto(a) do(a) Agente Responsável pela ETIR:

I — substituir o(a) Agente Responsável pela ETIR em seus impedimentos e ausências, assumindo integralmente as atribuições previstas no art. 15 desta Portaria;

II — receber notificações, prevenir, efetuar análise, investigar e conter incidentes que envolvam firewalls, sistemas de detecção e prevenção de intrusão, antivírus, proxies, servidores, Active Directory, DNS, DHCP, soluções de SIEM, roteadores, switches, VoIP, tecnologias de armazenamento e processamento de informações, elementos de conectividade, estações de trabalho, sistemas operacionais, ambientes de nuvem, data center, banco de dados e demais soluções tecnológicas de segurança da informação e de infraestrutura sob sua Gerência;

III — apoiar o tratamento de incidentes em sistemas, especialmente quando houver comprometimento de componentes de infraestrutura que suportem aplicações e serviços críticos do Tribunal; e

IV — recomendar ações para tomada de decisão na recuperação do ambiente após incidentes.

Art. 17. São atribuições do(a) Coordenador(a) de Cibersegurança:

I — executar, sob a orientação do(a) Agente Responsável ou do(a) Gerente de Cibersegurança e Ambientes Tecnológicos, as ações técnicas de monitoramento, análise, contenção e erradicação de ameaças no âmbito das ferramentas e tecnologias de segurança da informação;

II — coordenar a atuação dos(as) integrantes do Grupo de Apoio Técnico Especializado durante a execução das ações de resposta, conforme determinação do(a) Agente Responsável;

III — apoiar a elaboração de relatórios técnicos de incidentes, análises forenses e documentação de evidências digitais; e

IV — recomendar ações para tomada de decisão na recuperação de incidentes.

Art. 18. São atribuições do(a) Diretor(a) de Sistemas:

I — receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam sistemas judiciais de primeiro e segundo grau, sistemas administrativos, ambientes de desenvolvimento e sustentação de soluções e demais sistemas sob sua gestão;

II — mobilizar as gerências e coordenações subordinadas à Diretoria de Sistemas, conforme a natureza do incidente, assegurando a disponibilidade dos recursos técnicos e humanos necessários à resposta;

III — apoiar o tratamento de incidentes que envolvam vulnerabilidades em código-fonte, falhas em integrações entre sistemas ou comprometimento de ambientes de desenvolvimento; e

IV — recomendar ações para tomada de decisão na recuperação dos incidentes.

Art. 19. São atribuições do(a) Diretor(a) de Tecnologia do PJe:

I — receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam o Processo Judicial Eletrônico, incluindo seus módulos, integrações, fluxos, infraestrutura dedicada e bases de dados associadas;

II — mobilizar as gerências e coordenações subordinadas à Diretoria de Tecnologia do PJe, conforme a natureza do incidente, assegurando a disponibilidade dos recursos técnicos e humanos necessários à resposta;

III — apoiar o tratamento de incidentes em sistemas e infraestrutura que impactem a disponibilidade, a integridade ou a confidencialidade do PJe; e

IV — recomendar ações para tomada de decisão na recuperação dos incidentes.

Art. 20. São atribuições do(a) Diretor(a) de Inteligência Artificial e Plataformas Digitais:

I — receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam plataformas de dados, pipelines de ingestão e extração de dados, modelos de inteligência artificial, robôs de automação, automações inteligentes e demais soluções sob sua gestão;

II — mobilizar as gerências e coordenações subordinadas à Diretoria de Inteligência Artificial e Plataformas Digitais, conforme a natureza do incidente, assegurando a disponibilidade dos recursos técnicos e humanos necessários à resposta;

III — apoiar o tratamento de incidentes que envolvam comprometimento de credenciais de serviço utilizadas por automações, envenenamento ou manipulação de dados em plataformas de dados, comportamento anômalo de modelos de IA ou exfiltração de dados por meio de APIs;

IV — subsidiar a avaliação de impacto à proteção de dados pessoais quando o incidente envolver bases de dados sob sua gestão, em articulação com o(a) Coordenador(a) Estratégico(a) da ETIR; e

V — recomendar ações para tomada de decisão na recuperação dos incidentes.

Art. 21. São atribuições do(a) Gerente de Informática do Fórum Clóvis Beviláqua:

I — receber notificações, prevenir, efetuar análise, investigar e conter incidentes ocorridos ou que envolvam sistemas, aplicações, elementos de rede local e demais recursos de tecnologia da informação instalados no Fórum Clóvis Beviláqua;

II — atuar como ponto focal da ETIR no Fórum Clóvis Beviláqua, garantindo a comunicação tempestiva entre a equipe local e o(a) Agente Responsável sobre eventos e incidentes detectados naquela unidade;

III — apoiar o tratamento de incidentes em sistemas de primeiro grau que se manifestem no ambiente do Fórum; e

IV — recomendar ações para tomada de decisão na recuperação dos incidentes.

CAPÍTULO V

DOS SERVIÇOS E DA DOCUMENTAÇÃO DE INCIDENTES

Art. 22. Constituem serviços prestados pela ETIR:

I — tratamento de incidentes de segurança da informação: receber, filtrar, classificar e responder às solicitações e alertas, realizar a análise dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;

II — tratamento de artefatos maliciosos: receber informações ou cópia de artefato malicioso utilizado em ataque ou em qualquer atividade desautorizada, analisando sua natureza, mecanismo, versão e objetivo, para desenvolver ou sugerir estratégia de detecção, remoção e defesa;

III — tratamento de vulnerabilidades: receber informações sobre vulnerabilidades em hardware ou software, analisando sua natureza, mecanismo e consequências, e desenvolver estratégias para detecção e correção;

IV — emissão de alertas e advertências: divulgar alertas ou advertências como reação diante de incidente de segurança ou ameaça identificada, com o objetivo de orientar a comunidade de usuários(as) sobre as medidas a serem adotadas;

V — análise forense digital: coletar, preservar, analisar e documentar evidências digitais relacionadas a incidentes de segurança da informação, em apoio a investigações administrativas, auditorias ou procedimentos judiciais, quando determinado pelo(a) Coordenador(a) Estratégico(a) ou pelo CGSICCPDP;

VI — melhoria contínua: criar, revisar e propor melhorias nos processos, protocolos e procedimentos de prevenção, detecção e tratamento de incidentes de segurança da informação.

Art. 23. Os incidentes classificados nos níveis 3 (Alto) e 4 (Crítico) deverão ser formalmente documentados pelo(a) Agente Responsável pela ETIR, mediante a elaboração dos seguintes documentos:

I — Relatório de Comunicação de Incidente de Segurança, contendo, no mínimo, a descrição do incidente, a classificação de severidade, os ativos e dados afetados, as ações de contenção e recuperação adotadas, a linha do tempo dos eventos e as recomendações de melhoria;

II — Termo de Custódia dos Ativos de Informação relacionados ao incidente, documentando a cadeia de custódia das evidências digitais coletadas, em conformidade com os modelos previstos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

Parágrafo único. Para incidentes classificados nos níveis 1 (Baixo) e 2 (Médio), será obrigatório o registro no sistema de gestão de incidentes, contendo, no mínimo, a descrição do evento, a classificação, as providências adotadas e o encerramento.

CAPÍTULO VI

DOS CANAIS DE COMUNICAÇÃO

Art. 24. A notificação de incidentes de segurança da informação à ETIR poderá ser realizada pelos seguintes canais:

I — correio eletrônico: etir@tjce.jus.br;

II — correspondências oficiais por meio do Sistema Eletrônico de Informações (SEI);

III — comunicação presencial, em casos emergenciais;

IV — ferramentas tecnológicas de monitoramento e detecção de eventos de segurança; e

V — sistema de chamados técnicos em uso pelo Tribunal.

CAPÍTULO VII

DA CAPACITAÇÃO

Art. 25. O(A) agente responsável pela ETIR promoverá programa de capacitação periódica para os(as) integrantes da equipe, abrangendo, no mínimo:

I — gestão e resposta a incidentes de segurança da informação;

II — análise forense digital e preservação de evidências;

III — proteção de dados pessoais e direitos dos(as) titulares; e

IV — conhecimento dos protocolos e manuais aprovados pela Portaria CNJ nº 162/2021.

§1º A capacitação de que trata o caput será realizada ao menos uma vez por ano e sempre que houver alteração significativa nos procedimentos ou na composição da ETIR.

§2º A Diretoria de Segurança da Informação (DSI) buscará, junto à Alta Administração, os meios necessários para viabilizar a participação dos(as) integrantes da ETIR nas referidas capacitações, conforme disponibilidade orçamentária.

CAPÍTULO VIII

DOS INDICADORES DE DESEMPENHO

Art. 26. O(A) Coordenador(a) Estratégico(a) da ETIR, em articulação com o(a) Agente Responsável, definirá e acompanhará indicadores de desempenho para a avaliação da efetividade da resposta a incidentes, incluindo, no mínimo:

I — tempo médio de detecção de incidentes (Mean Time to Detect - MTDD);

II — tempo médio de contenção de incidentes (Mean Time to Contain - MTTC);

III — tempo médio de recuperação de incidentes (Mean Time to Recover - MTTR);

IV — quantidade de incidentes por nível de severidade em período determinado;

V — percentual de incidentes encerrados dentro dos prazos definidos nos procedimentos operacionais.

Parágrafo único. Os indicadores de que trata o caput serão reportados ao CGSICCPDP com periodicidade semestral, ou em menor periodicidade quando solicitado pelo Comitê, e subsidiarão a avaliação do nível de maturidade em segurança cibernética do Tribunal, conforme previsto no art. 12, inciso III, da Resolução CNJ nº 396/2021.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 27. 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, trabalhando em articulação com as demais unidades envolvidas para a tomada de decisão sobre as medidas a serem adotadas.

Art. 28. O CGSICCPDP expedirá ato complementar definindo a composição inicial do Grupo de Apoio Técnico Especializado, ouvidos(as) o(a) Secretário(a) de Tecnologia da Informação e o(a) Diretor(a) do Fórum Clóvis Beviláqua.

Art. 29. O plano de Resposta a Incidentes de Segurança da Informação, previsto no art. 3º, inciso III, e detalhado no art. 6º desta Portaria, será elaborado ou revisado pela ETIR no prazo de 120 (cento e vinte) dias a contar da publicação desta Portaria, para adequação à nova estrutura, aos procedimentos nela estabelecidos e à integração com o Plano de Continuidade de Negócio e o Plano de Recuperação de Desastres do Tribunal.

Art. 30. As referências a resoluções, portarias, protocolos e manuais editados pelo Conselho Nacional de Justiça (CNJ) contidas nesta Portaria compreendem as normas vigentes à data de sua publicação e quaisquer atos normativos supervenientes que os revoguem, alterem, complementem ou substituam, aplicando-se automaticamente as disposições da norma mais recente, independentemente de revisão formal deste ato.

Parágrafo único. Caso a norma superveniente introduza obrigações, estruturas ou procedimentos incompatíveis com o disposto nesta Portaria, o(a) Coordenador(a) Estratégico(a) da ETIR comunicará o fato ao CGSICCPDP no prazo de 30 (trinta) dias a contar da publicação da norma superveniente, instruindo a comunicação com análise de impacto e proposta de adequação.

Art. 31. Sem prejuízo da recepção automática prevista no art. 30, esta Portaria será objeto de revisão formal sempre que a norma superveniente introduzir obrigações incompatíveis com o aqui disposto, quando houver alteração organizacional relevante na estrutura do Tribunal, e, em qualquer caso, em prazo não superior a 2 (dois) anos contados da sua publicação ou da última revisão.

Art. 32. Fica revogada a Portaria nº 1820/2022, de 17 de agosto de 2022, da Presidência do Tribunal de

Justiça do Estado do Ceará.

Art. 33. Esta Portaria entra em vigor na data de sua publicação.

REGISTRE-SE, PUBLIQUE-SE E CUMPRA-SE.

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, em Fortaleza, aos 29 (vinte e nove) dias do mês de setembro de 2026.

Desembargador Heráclito Vieira de Sousa Neto

Presidente do Tribunal de Justiça do Estado do Ceará

Para visualizar a matéria completa, acesse o link <https://djea-con.tjce.jus.br/materias/179935> ou realize a leitura do QR-Code ao lado.

