

TRIBUNAL DE JUSTIÇA - ATOS DO PRESIDENTE

PORTARIA 02302/2026

Disponibilização: 29/09/2026 às 16h20m

PORTARIA Nº 2302/2026-GABPRESI

Institui procedimentos e diretrizes para prevenção, detecção e tratamento de códigos maliciosos 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 o aumento e a sofisticação dos ataques cibernéticos que impactam todos os setores da sociedade, com potenciais prejuízos operacionais, financeiros, reputacionais e jurídicos, e a consequente necessidade de proteção contínua para assegurar a disponibilidade dos serviços digitais do Poder Judiciário;

CONSIDERANDO a necessidade de adoção permanente e padronizada de medidas técnicas e administrativas de prevenção, detecção e tratamento de códigos maliciosos, com vistas a mitigar riscos de interrupção de serviços, indisponibilidade de sistemas e perda de dados, assegurando a integridade dos ativos tecnológicos e a continuidade dos serviços;

CONSIDERANDO o disposto na Resolução do Conselho Nacional de Justiça (CNJ) nº 396, de 7 de junho de 2021, republicada em 24 de setembro de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), em especial os objetivos de aumentar a resiliência às ameaças cibernéticas e de permitir a manutenção e a continuidade dos serviços judiciais;

CONSIDERANDO o disposto na Portaria CNJ nº 162, de 10 de junho de 2021, que aprova os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO o disposto na Portaria do TJCE nº 2521/2022, que estabelece os protocolos de prevenção de incidentes, gerenciamento de crises cibernéticas e investigação para ilícitos cibernéticos do Poder Judiciário do Estado do Ceará;

CONSIDERANDO o disposto na Resolução do Órgão Especial do TJCE nº 15/2023, que regulamenta a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Ceará, com as alterações introduzidas pela Resolução do Órgão Especial nº 21/2024;

CONSIDERANDO o disposto na Resolução do Órgão Especial nº 03/2023, com as alterações introduzidas pela Resolução do Órgão Especial nº 11/2025, que instituiu o Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP) no âmbito do Poder Judiciário do Estado do Ceará;

CONSIDERANDO o disposto na Portaria nº 1186/2018, que estabelece, no âmbito do Poder Judiciário do Estado do Ceará, o conjunto de normas complementares à Política de Segurança da Informação, ao qual se vincula a presente Norma para Tratamento de Códigos Maliciosos, na qualidade de revisão e substituição da

redação anteriormente vigente do seu Anexo IV.

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer as diretrizes e os procedimentos para prevenção, detecção e tratamento de códigos maliciosos no âmbito do Poder Judiciário do Estado do Ceará.

Art. 2º Esta norma aplica-se a todas as unidades administrativas e judiciais, bem como a magistrados(as), servidores(as), colaboradores(as), estagiários(as), prestadores(as) de serviço, fornecedores(as) e demais pessoas físicas ou jurídicas que utilizem, administrem ou tenham acesso aos ativos tecnológicos do Poder Judiciário do Estado do Ceará, observada, no que couber, a definição de Usuário constante do art. 3º, inciso I.

Art. 3º Para fins desta Norma, considera-se:

I – Usuário: magistrados(as) e servidores(as) ocupantes de cargo efetivo ou em comissão, requisitados(as) e cedidos(as), desde que previamente autorizados(as), empregados(as) de empresas prestadoras de serviços terceirizados, conveniados(as), consultores(as), estagiários(as) e demais pessoas que se encontrem a serviço da Justiça Estadual, utilizando os recursos tecnológicos do Poder Judiciário do Estado do Ceará;

II – Códigos Maliciosos: programas, scripts ou rotinas projetadas para causar danos, explorar vulnerabilidades ou permitir acesso não autorizado a sistemas e dados, com potencial de comprometer a disponibilidade, integridade ou confidencialidade das informações;

III – Vírus: programa malicioso que se propaga inserindo cópias de si mesmo em outros programas ou arquivos, alterando seu funcionamento original;

IV – Cavalo de Tróia: programa aparentemente legítimo que, além da função esperada, executa ações maliciosas sem o conhecimento do usuário, podendo instalar outros códigos maliciosos ou criar portas de acesso não autorizadas;

V – Spyware: software que monitora atividades de um sistema e envia as informações coletadas a terceiros, sem autorização do usuário, violando a privacidade e a segurança institucional;

VI – Backdoors: mecanismo ou programa que cria canais ocultos para o retorno de invasores a um sistema comprometido, contornando processos regulares de autenticação;

VII – Keylogger: programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador;

VIII – Worm: programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador;

IX – Bot: programa automatizado que, após infectar um dispositivo, permite sua operação remota sem o

consentimento do usuário, podendo integrar redes de ataque coordenadas;

X – Botnet: rede de dispositivos comprometidos (bots) controlados remotamente por agentes maliciosos, normalmente utilizada em ataques de negação de serviço ou disseminação de spam;

XI – Rootkit: conjunto de ferramentas utilizadas para ocultar a presença e as atividades de invasores em um sistema comprometido, assegurando acesso persistente e não autorizado;

XII – Log: arquivo que contém informações sobre eventos de qualquer natureza ocorridos em um sistema computacional, utilizado para análise forense de incidentes de segurança, auditoria de processos, cumprimento de exigências legais relativas à manutenção do registro do histórico de acessos ou eventos e para a resolução de problemas;

XIII – MITRE ATT&CK: base de conhecimento globalmente acessível sobre táticas e técnicas de adversários, baseada em observações do mundo real, usada como fundamento para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de cibersegurança;

XIV – Antimalware: ferramenta de segurança destinada à prevenção, detecção e remoção de programas maliciosos, devendo ser instalada e mantida atualizada em todos os ativos de tecnologia do Poder Judiciário, abrangendo, para fins desta norma, as soluções tradicionais de antimalware e as soluções de detecção e resposta em endpoint (EDR/XDR), conforme inciso XVIII;

XV – Firewall de Perímetro: sistema de segurança que realiza o controle de tráfego entre redes internas e externas, permitindo ou bloqueando comunicações de acordo com políticas definidas pela área de tecnologia da informação;

XVI – Web Application Firewall (WAF): solução de firewall de aplicações que protege aplicações web e APIs contra ataques e tentativas de exploração de vulnerabilidades, monitorando e filtrando o tráfego HTTP e HTTPS;

XVII – Ransomware: código malicioso que bloqueia o acesso a dados ou sistemas mediante criptografia, exigindo pagamento de resgate para sua liberação;

XVIII – Endpoint/Extended Detection and Response (EDR/XDR): soluções tecnológicas voltadas à detecção e resposta automatizada a ameaças cibernéticas em dispositivos, redes e servidores institucionais.

CAPÍTULO II

DAS DIRETRIZES PARA O FUNCIONAMENTO E A OPERAÇÃO DOS SERVIÇOS DE TRATAMENTO DE CÓDIGOS MALICIOSOS

Art. 4º Todas as estações de trabalho, notebooks, servidores e demais ativos tecnológicos compatíveis com a solução de antimalware adotada pelo Poder Judiciário do Estado do Ceará deverão possuir a proteção instalada, habilitada e devidamente atualizada.

Parágrafo único. Quando não for possível a instalação da solução de antimalware em razão de

incompatibilidade técnica do sistema operacional ou de aplicação legada, deverão ser adotados controles compensatórios e mecanismos de endurecimento (hardening) que reduzam o nível de exposição ao risco do ativo.

Art. 5º A solução de antimalware deverá atualizar automaticamente os mecanismos de proteção contra códigos maliciosos conforme novas versões estejam disponíveis.

Art. 6º As atualizações de segurança dos serviços de antimalware deverão ser implementadas de maneira automática e recorrente, de modo a evitar vulnerabilidades nos sistemas que devem ser protegidos.

Parágrafo único. Atualizações que possam afetar sistemas ou processos críticos deverão ser executadas por meio do processo formal de Gestão de Mudanças.

Art. 7º Em caso de incidente cibernético decorrente de malware, os procedimentos adotados para tratamento e resposta deverão ser executados conforme o Plano de Gestão de Incidentes de Segurança da Informação e demais normativos institucionais aplicáveis.

Art. 8º Os serviços de antimalware, firewall de perímetro e Web Application Firewall (WAF) deverão ser configurados para executar, de forma automática, as cópias de segurança do banco de dados e das respectivas configurações, em periodicidade definida em procedimento operacional próprio aprovado pela Coordenadoria de Cibersegurança.

§1º As cópias de segurança deverão ser armazenadas em local seguro, segregado do ambiente de produção e com alta disponibilidade.

§2º O procedimento operacional referido no caput estabelecerá, para cada serviço, a ferramenta ou o mecanismo responsável pela execução e pela guarda das cópias de segurança, observada, no que couber, a Norma Geral para Cópias de Segurança da Informação do TJCE.

Art. 9º Caso um agente de antimalware detecte a presença de artefato malicioso, o arquivo deverá ser imediatamente colocado em quarentena ou ter sua execução bloqueada de forma automática.

Parágrafo único. A análise e a classificação manual do evento, com registro formal da ocorrência, serão obrigatórias quando:

I – a remediação automática falhar;

II – o artefato for classificado como crítico ou severo pelo agente; ou

III – houver suspeita de comprometimento do ativo.

Art. 10. As soluções de antimalware implementadas nos ambientes de homologação e teste deverão observar a paridade de configurações, perfis e versões em relação ao ambiente de produção, a fim de assegurar a fidedignidade dos testes e prevenir incidentes ou indisponibilidades durante a promoção de serviços para o ambiente produtivo, decorrentes de divergências de segurança.

Art. 11. As configurações e políticas aplicadas nos serviços de segurança, incluindo antimalware, firewall de perímetro e WAF, deverão ser avaliadas e auditadas periodicamente, de modo a assegurar sua conformidade, eficácia e alinhamento contínuo às boas práticas recomendadas pelos fabricantes e aos principais referenciais

internacionais de segurança da informação, como os CIS Benchmarks, as publicações da série NIST SP 800, o MITRE ATT&CK Framework e a ISO/IEC 27002, garantindo aderência aos controles técnicos definidos nesta Norma.

CAPÍTULO III

DAS PROTEÇÕES CONFIGURADAS CONTRA CÓDIGOS MALICIOSOS NA SOLUÇÃO DE ANTIMALWARE

Art. 12. O serviço de antimalware vigente deverá ter as suas funções habilitadas de acordo com o:

- I – o tipo de sistema operacional;
- II – as características das aplicações utilizadas no ativo;
- III – o nível de criticidade do ativo; e
- IV – as ameaças que possam explorar vulnerabilidades do ativo.

Art. 13. O serviço de antimalware deverá ser configurado para proteger o ativo em relação a possíveis ameaças internas ou externas, cabendo à área responsável configurar e preservar de maneira permanente a disponibilidade e o desempenho do servidor ou da estação de trabalho gerenciada.

Art. 14. O sistema de proteção contra códigos maliciosos deverá utilizar seus recursos técnicos para assegurar a visibilidade e a integridade do ambiente digital, observando as seguintes configurações:

I – Monitoramento e análise:

- a) a solução deverá monitorar continuamente e analisar, de forma correlacionada, diretamente ou em integração com a plataforma de gerenciamento de eventos de segurança (SIEM) institucional;
- b) monitoramento dos estados de execução dos processos e as modificações em arquivos do sistema operacional;
- c) monitoramento do tráfego de rede e o conteúdo de códigos executados em nível de memória;
- d) análise do comportamento de usuários e serviços, visando identificar atividades anômalas; e
- e) detecção das técnicas e táticas de ataque descritas na matriz MITRE ATT&CK.

II – Identificação e detecção:

- a) identificação de arquivos e anexos provenientes de serviços de nuvem, correio eletrônico e plataformas de produtividade (ex.: Microsoft 365), no momento de sua gravação, abertura ou execução nos ativos gerenciados;
- b) identificação URLs, domínios e artefatos classificados como maliciosos ou destinados a campanhas de phishing.

III – Bloqueio e resposta:

a) bloqueio e interrupção de ransomwares, keyloggers, bots, vírus, cavalos de troia, spywares, backdoors e demais variantes de códigos maliciosos;

b) bloqueio de ameaças identificadas por meio de análise comportamental ou assinaturas de segurança.

§1º A implementação dos recursos previstos neste artigo observará as capacidades técnicas das soluções efetivamente licenciadas e contratadas pelo TJCE.

§2º As funcionalidades previstas neste artigo que não estejam disponíveis no parque tecnológico vigente deverão ser formalmente registradas no processo de Gestão de Riscos de TIC, com indicação dos controles compensatórios adotados e, quando cabível, do plano de adequação.

Art. 15. O sistema de antimalware deverá empregar métodos de detecção baseados em assinaturas e algoritmos de aprendizado de máquina para identificação de ameaças emergentes.

Art. 16. Com o objetivo de conter um ataque iminente ou em curso, o sistema de antimalware deverá ser capaz de realizar o isolamento de rede de ativos gerenciados.

§1º O isolamento automático ficará restrito aos ativos individuais que apresentem indícios de comprometimento, conforme critérios técnicos definidos em procedimento operacional próprio.

§2º O isolamento simultâneo de múltiplos ativos ou da totalidade dos ativos gerenciados somente poderá ser executado de forma manual, mediante decisão motivada da Coordenadoria de Cibersegurança, com comunicação imediata à Gerência de Cibersegurança e Ambientes Tecnológicos e à Diretoria de Segurança da Informação.

§3º A adoção das medidas previstas neste artigo deverá observar o Plano de Gestão de Incidentes de Segurança da Informação e ponderar o impacto sobre a disponibilidade dos serviços judiciais, em atenção ao objetivo de continuidade dos serviços previsto na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (Resolução CNJ nº 396/2021).

Art. 17. O sistema de antimalware deverá ter a função de detectar e prevenir a utilização de sítios eletrônicos ou domínios categorizados como maliciosos, complementando as camadas de proteção com o serviço de filtro executado pelo firewall de perímetro.

Art. 18. Para evitar a execução de código malicioso de forma automática, devem ser desabilitados o autorun e o autoplay para dispositivo USB e outras mídias similares através do sistema de antimalware ou por algum outro meio técnico equivalente.

Art. 19. As mídias removíveis autorizadas que são utilizadas nas estações de trabalho e notebooks do TJCE deverão ser submetidas à verificação automática pelo sistema de antimalware antes de seu uso.

CAPÍTULO IV

DAS PROTEÇÕES CONTRA CÓDIGOS MALICIOSOS NO SERVIÇO DE FIREWALL DE PERÍMETRO

Art. 20. O firewall de perímetro deverá ser configurado para detectar e prevenir, nas conexões de rede, a execução ou propagação de código malicioso.

Art. 21. O firewall de perímetro deverá inspecionar o tráfego de rede das seguintes origens e destinos:

I - Internet;

II - redes internas;

III - conexões VPNs site-to-site; e

IV - conexões VPNs client-to-site.

Art. 22. As regras de proteção configuradas no firewall de perímetro deverão contemplar, observadas as características e os riscos de cada ambiente, as seguintes funcionalidades:

I - inspeção às portas TCP/UDP conhecidas;

II - detecção e bloqueio de possíveis vulnerabilidades conhecidas que exploram falhas no conjunto de protocolos TCP/IP;

III - detecção e mitigação de varredura de portas, DoS e DDoS;

IV - detecção de presença de arquivos maliciosos em trânsito nas conexões de rede;

V - descoberta de ataques, como buffer overflow, execução remota de código, fragmentação e obfuscação; e

VI - descryptografia seletiva das conexões HTTPS, visando identificar possíveis conexões ou artefatos maliciosos, observado o disposto no §3º deste artigo.

§1º Confirmada a ocorrência de ação maliciosa em curso, a conexão deverá ser bloqueada de forma imediata, persistindo o bloqueio até a conclusão da análise técnica e a adoção das medidas de remediação cabíveis.

§2º As configurações de proteção que devem estar habilitadas em cada regra de proteção dependem de fatores como:

I - tipo de tráfego;

II - ativos que fazem parte da regra;

III - aspectos legais de uma possível interceptação de tráfego por meio da descryptografia das conexões via protocolo HTTPS;

IV - possíveis ameaças; e

V - fatores como o processamento e o uso de memória do appliance físico ou virtual.

§3º A descriptografia de conexões HTTPS:

I – será aplicada de forma seletiva, por categorias de tráfego e de ativos definidas em procedimento operacional aprovado pela Diretoria de Segurança da Informação;

II – excluirá, sempre que tecnicamente identificáveis, as categorias de tráfego protegidas por sigilo legal ou profissional, tais como serviços de saúde, instituições financeiras e comunicações resguardadas por prerrogativa profissional;

III – observará a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), limitando-se ao estritamente necessário à finalidade de segurança da informação, vedada a sua utilização para monitoramento de conteúdo de natureza pessoal dos usuários;

IV – terá sua aplicação registrada de forma auditável, com ciência do encarregado pelo tratamento de dados pessoais do TJCE quanto ao procedimento adotado.

CAPÍTULO V

DAS PROTEÇÕES CONTRA CÓDIGOS MALICIOSOS NO WEB APPLICATION FIREWALL (WAF)

Art. 23. O Web Application Firewall (WAF) deverá ser configurado, por padrão, para bloquear o upload de arquivos executáveis ou potencialmente perigosos para qualquer diretório ou caminho de aplicação, sistema, site ou API sob sua proteção.

Art. 24. O WAF deverá ser configurado para identificar, analisar e bloquear requisições web que contenham padrões conhecidos de códigos maliciosos, incluindo, mas não se limitando a:

I – SQL Injection;

II – OS Command Injection;

III – Cross-Site Scripting – XSS;

IV – Server-Side Template Injection;

V – XML External Entity – XXE;

VI – Insecure Deserialization;

VII – Local/Remote File Inclusion – LFI/RFI;

VIII – Web-shell e scripts remotos;

IX – Server-Side Request Forgery – SSRF; e

X – HTTP Header / Parameter Pollution.

§1º As proteções descritas neste capítulo aplicam-se às aplicações, sistemas e APIs formalmente integrados ao serviço de WAF.

§2º Deverão ser obrigatoriamente integrados ao serviço de WAF, ressalvada motivação técnica formalmente registrada e aprovada pela Diretoria de Segurança da Informação, mediante justificativa técnica e análise de risco:

I – os sistemas e aplicações de acesso público externo;

II – os sistemas e aplicações que tratem dados pessoais ou dados pessoais sensíveis; e

III – os sistemas e aplicações classificados como críticos pelo processo de classificação de ativos do TJCE.

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 25. Compete à Diretoria de Segurança da Informação:

I – exercer a governança institucional sobre o tratamento de códigos maliciosos no âmbito do Poder Judiciário do Estado do Ceará, supervisionando o cumprimento desta norma pelas unidades a ela vinculadas;

II – aprovar formalmente as exceções às regras estabelecidas nesta Norma, mediante justificativa técnica e análise de risco, com ciência do Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP);

III – conduzir, ou determinar a condução, das auditorias formais sobre os controles, configurações e serviços de antimalware/EDR, firewall de perímetro e WAF, podendo, para tanto, articular-se com a Secretaria de Auditoria Interna do TJCE;

IV – atuar como interlocutor formal do TJCE junto ao CGSICCPDP, à Secretaria de Tecnologia da Informação (SETIN) e a órgãos externos, em matéria de tratamento de códigos maliciosos; e

V – avaliar, no mínimo anualmente, os indicadores de efetividade dos controles desta norma, com base nos relatórios encaminhados pela Coordenadoria de Cibersegurança, e propor medidas de aprimoramento.

Art. 26. Compete à Gerência de Cibersegurança e Ambientes Tecnológicos, vinculada à Secretaria de Tecnologia da Informação:

I – supervisionar a instalação, a atualização e a operação contínua das soluções de antimalware/EDR, firewall de perímetro e WAF nos ativos tecnológicos sob sua gestão, em conformidade com as diretrizes do fabricante e as diretrizes institucionais de segurança, assegurando a correta operação;

II – avaliar o desempenho e possíveis problemas encontrados nos servidores, decorrentes de novas funcionalidades ou de mudanças ocorridas dentro dos serviços de antimalware, firewall de perímetro e WAF, garantindo que não comprometam a disponibilidade ou integridade dos sistemas corporativos;

III - articular-se com a Coordenadoria de Suporte para que as estações de trabalho estejam com o software de proteção instalado e atualizado antes da entrega ou reinstalação dos equipamentos aos usuários;

IV - supervisionar a manutenção do registro estruturado de eventos e incidentes mantido pela Coordenadoria de Cibersegurança e validar os relatórios periódicos encaminhados à Diretoria de Segurança da Informação;

V - garantir a instalação e a correta operação do antimalware em todas as estações de trabalho/os servidores compatíveis; e

VI - certificar-se de que as estações de trabalho dos servidores estejam com o software de proteção atualizado antes da entrega ou reinstalação dos equipamentos aos usuários.

Art. 27. Compete à Coordenadoria de Cibersegurança, vinculada à Secretaria de Tecnologia da Informação:

I - executar a instalação e assegurar a operação contínua da solução de antimalware/EDR nos ativos tecnológicos sob a gestão da Gerência de Cibersegurança e Ambientes Tecnológicos;

II - gerenciar de maneira contínua os serviços de antimalware, firewall de perímetro e o WAF;

III - monitorar os eventos gerados pelos serviços de firewall de perímetro, antimalware e o WAF por meio de um Gerenciamento de Informações e Eventos de Segurança (SIEM), com o objetivo de atuar de maneira proativa na identificação e investigação de incidentes;

IV - coordenar a contenção e erradicação dos códigos maliciosos identificados e não tratados automaticamente pelos sistemas de segurança;

V - configurar e ativar os mais diferentes filtros de proteção a nível de firewall de perímetro e WAF para as conexões de saída e entrada;

VI - realizar verificações internas e análises periódicas de conformidade técnica sobre os controles, as configurações de segurança e a efetividade operacional dos serviços de antimalware/EDR, firewall de perímetro e WAF sob sua gestão, com registro formal das constatações em relatórios técnicos e adoção das medidas corretivas pertinentes, sem prejuízo das auditorias formais a serem conduzidas pela Diretoria de Segurança da Informação ou pela Auditoria Interna do TJCE;

VII - executar a cópia de segurança do banco de dados e das configurações dos serviços de antimalware, firewall de perímetro e WAF, em periodicidade definida em procedimento operacional próprio, armazenando-as em ambiente seguro;

VIII - elaborar e manter procedimentos e documentações que detalhem a instalação, atualização e operação do software de antimalware para todas as versões dos sistemas operacionais compatíveis com o serviço;

IX - promover, em articulação com as áreas competentes, a conscientização e o treinamento contínuo dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos e engenharia social; e

X - manter registro estruturado e auditável de todos os eventos e incidentes envolvendo códigos maliciosos detectados pelos serviços de antimalware/EDR, firewall de perímetro e WAF, abrangendo tanto os tratados por

remediação automática quanto os submetidos à análise manual, contendo, no mínimo:

- a) identificação do ativo afetado;
- b) data e hora da detecção;
- c) vetor de infecção;
- d) classificação de severidade;
- e) medidas técnicas adotadas;
- f) status de resolução; e
- g) lições aprendidas, quando aplicável.

Parágrafo único. A Coordenadoria de Cibersegurança encaminhará à Diretoria de Segurança da Informação relatórios periódicos consolidados, em frequência definida em procedimento operacional próprio, sem prejuízo da comunicação imediata exigida em casos de incidente crítico.

Art. 28. Compete aos Usuários:

- I - reportar, através das ferramentas oficiais, mensagens suspeitas, possíveis casos de phishing e arquivos maliciosos recebidos por e-mail;
- II - cumprir integralmente as boas práticas aprendidas através dos treinamentos e campanhas de conscientização recorrentes; e
- III - reportar imediatamente qualquer infecção ou suspeita de infecção por código malicioso.

Art. 29. Compete aos fornecedores e prestadores de serviço:

- I - cumprir integralmente os requisitos e procedimentos estabelecidos nesta Norma, observando as cláusulas contratuais de confidencialidade e segurança da informação;
- II - notificar imediatamente à Coordenadoria de Cibersegurança qualquer incidente ou indício de código malicioso detectado durante a prestação de serviços;
- III - observar que os contratos firmados com terceiros e fornecedores que envolvam acesso à rede, sistemas, dados ou ambientes do TJCE, celebrados a partir da publicação desta Norma, bem como os respectivos aditivos celebrados após sua vigência, deverão conter cláusulas específicas de conformidade com esta Norma, com a Política de Segurança da Informação e com os requisitos mínimos de segurança cibernética nas contratações, em atenção à Resolução CNJ nº 396/2021 e aos normativos correlatos do TJCE.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS E DAS PENALIDADES

Art. 30. Detectada, por meio dos serviços de antimalware/EDR, firewall de perímetro ou WAF, a utilização, o download, a execução ou a transferência de qualquer código malicioso, a Coordenadoria de Cibersegurança conduzirá análise técnica do evento, com o objetivo de identificar o vetor de infecção, a extensão do comprometimento e a causa imediata da ocorrência.

§1º Durante a análise, o acesso do usuário poderá ser preventivamente restringido por decisão motivada da Coordenadoria de Cibersegurança, com comunicação imediata ao próprio usuário, observado o princípio da proporcionalidade e adotando-se medidas para conter o risco.

§2º A chefia imediata do usuário será comunicada quando configurada qualquer das seguintes hipóteses:

I – a análise técnica indicar indícios de conduta dolosa, fraudulenta ou de negligência grave por parte do usuário;

II – houver reincidência do mesmo usuário;

III – o usuário se recusar a colaborar com a análise técnica ou a adotar as medidas corretivas indicadas; ou

IV – o evento for classificado pela Coordenadoria de Cibersegurança como crítico ou severo, nos termos desta Norma, em razão da extensão do comprometimento, da exposição de dados pessoais ou da continuidade dos serviços.

§3º Configurada qualquer das hipóteses do §2º, a Coordenadoria de Cibersegurança comunicará formalmente a ocorrência à chefia imediata e à diretoria correspondente, instruindo a comunicação com o relatório técnico do evento, para apuração nos termos da legislação aplicável.

Art. 31. O acesso aos recursos tecnológicos institucionais somente será restabelecido após a conclusão da análise técnica do evento e a adoção das medidas corretivas pertinentes, que poderão incluir, conforme o caso, orientação ao usuário, capacitação dirigida, atualização de configurações do ativo, substituição de credenciais e demais providências de remediação tecnicamente cabíveis.

Art. 32. O Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP) será informado dos incidentes e poderá determinar as providências administrativas cabíveis.

Art. 33. O descumprimento das disposições desta Norma poderá ensejar a adoção de medidas administrativas, incluindo bloqueio temporário ou definitivo de acesso aos recursos tecnológicos institucionais, cancelamento de credenciais de acesso, instauração de processo administrativo disciplinar, e, quando cabível, medidas cíveis ou criminais, conforme legislação vigente.

Art. 34. Toda e qualquer exceção às regras estabelecidas nesta Norma deverá ser previamente formalizada e autorizada pela Diretoria de Segurança da Informação, com ciência do Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP), mediante justificativa técnica e análise de risco que assegure não haver comprometimento da segurança institucional.

Art. 35. Esta Norma deverá ser revisada sempre que houver atualização tecnológica ou alteração significativa no ambiente computacional e, em qualquer caso, no mínimo a cada 2 (dois) anos, devendo ser submetida à

apreciação e aprovação do Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP).

Art. 36. Fica revogado o Anexo IV da Portaria nº 1186/2018, que dispõe sobre o Tratamento de Códigos Maliciosos no âmbito do Tribunal de Justiça do Estado do Ceará.

Art. 37. 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/179933> ou realize a leitura do QR-Code ao lado.

