# Diário da Justiça Eletrônico

Poder Judiciário de Pernambuco

Ano XVI Edição nº 142/2024 | Recife - PE, segunda-feira, 22 de julho de 2024

Disponibilização: 19/07/2024 | Publicação: 22/07/2024





## Composição do TJPE

| | |
|---|---|
| Des. Bartolomeu Bueno de Freitas Morais | Des. Eudes dos Prazeres França |
| Des. Frederico Ricardo de Almeida Neves | Des. Carlos Frederico Gonçalves de Moraes |
| Des. Adalberto de Oliveira Melo | Des. Fábio Eugênio Dantas de Oliveira Lima |
| Des. Fernando Cerqueira Norberto dos Santos | Des. Márcio Fernando de Aguiar Silva |
| Des. Luiz Carlos de Barros Figueiredo | Des. Humberto Costa Vasconcelos Júnior |
| Des. Alberto Nogueira Virgínio | Des. Waldemir Tavares de Albuquerque Filho |
| Des. Antônio Fernando Araújo Martins | Des. José Viana Ulisses Filho |
| Des. Ricardo de Oliveira Paes Barreto | Des. Sílvio Neves Baptista Filho |
| Des. Cândido José da Fonte Saraiva de Moraes | Des. Demócrito Ramos Reinaldo Filho |
| Des. Francisco José dos Anjos Bandeira de Mello | Des. Évio Marques da Silva |
| Des. Antenor Cardoso Soares Júnior | Des. Honório Gomes do Rego Filho |
| Des. Alexandre Guedes Alcoforado Assunção | Des. Ruy Trezena Patu Júnior |
| Des. Mauro Alencar de Barros | Des. Isaías Andrade Lins Neto |
| Des. Fausto de Castro Campos | Des. Paulo Romero de Sá Araújo |
| Des. Cláudio Jean Nogueira Virgínio | Des. Gabriel de Oliveira Cavalcanti Filho |
| Des. Francisco Eduardo Gonçalves Sertório Canto | Des. Raimundo Nonato de Souza Braid Filho |
| Des. José Ivo de Paula Guimarães | Des. Eduardo Guilliod Maranhão |
| Des. Josué Antônio Fonseca de Sena | Des. Luiz Gustavo Mendonça de Araújo |
| Des. Agenor Ferreira de Lima Filho | Des. Paulo Augusto de Freitas Oliveira |
| Des. Jorge Américo Pereira de Lira | Des. Alexandre Freire Pimentel |
| Des. Erik de Sousa Dantas Simões | Des. Luciano de Castro Campos |
| Des. Stênio José de Sousa Neiva Coêlho | Desa.Valéria Bezerra Pereira Wanderley |
| Des. André Oliveira da Silva Guimarães | Des. Paulo Roberto Alves da Silva |
| Des. Itamar Pereira da Silva Júnior | Des. André Vicente Pires Rosa |
| Des. Evandro Sérgio Netto de Magalhães Melo | Des. José Severino Barbosa |
| Desa. Daisy Maria de Andrade Costa Pereira | CARGO VAGO |


Palácio da Justiça - Praça da República, s/n
Santo Antônio - Recife - PE
CEP: 50010-040
**Telefones:** (81) 3182-0100
**Site:** www.tjpe.jus.br

**Dúvidas / Sugestões:** diario.eletronico@tjpe.jus.br
**Telefones:** (81) 3182.0643

**Coordenação e Gerenciamento:**
Carlos Gonçalves da Silva
Renata Ferraz Gomes

**Diretoria de Documentação Judiciária:**
Leidiane de Lacerda Silva
Carolina Tiemi de D Ishigami M Pereira
Edilson Ferreira da Silva

**Gerência de Jurisprudência e Publicações:**
Marcia Maria Ramalho da Silva

**Chefia da Unidade de Diário de Justiça Eletrônico:**
Natália Barros Costa

**Produção e Editoração:**
Natália Barros Costa

**Art. 18.** Cabe à ETIR identificar incidentes que possam indicar uma crise em potencial, informando-os ao Comitê de Crises Cibernéticas para posterior caracterização da crise.

**Art. 19.** O Comitê de Crises Cibernéticas reunir-se-á tão logo seja notificado pela ETIR, para avaliar a caracterização do incidente como crise.

**Art. 20.** Os planos de contingência e de tratamento devem ser aplicados tempestivamente, caso já existam, em um eventual cenário de incidentes em andamento, visando sempre a salvaguarda de pessoas, informações e bens materiais e a continuidade dos processos de negócio.

**CAPÍTULO IV**

**DO PÓS CRISE**

**Art. 21.** Ultrapassada a crise, após o retorno aos níveis normais de operação dos processos de negócio, cabe ao Comitê de Crises Cibernéticas:

**I** – analisar criticamente as ações tomadas durante a crise para identificar e registrar pontos de sucesso e necessidades de ajustes nos procedimentos;

**II** – elaborar relatório final interno, detalhando:

a) a identificação e análise da causa-raiz do incidente;

b) a linha do tempo das ações realizadas;

c) a escala do impacto nos dados, sistemas e operações de negócios;

d) os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas; o escalonamento da crise;

e) a investigação e preservação de evidências; a efetividade das ações de contenção;

f) a coordenação da crise, liderança das equipes e gerenciamento de informações;

g) a tomada de decisão e as estratégias de recuperação.

**Art. 22.** A revisão detalhada das ações executadas será utilizada para registro e para subsidiar a melhoria das estratégias e planos a serem executados em crises futuras.

**Art. 23.** Será elaborado Relatório de Comunicação de Incidente de Segurança Cibernética para diálogo com outros Órgãos do Judiciário por meio da rede colaborativa regida pelo CPTRIC-PJ, como disposto na Resolução CNJ nº 396/2021.

**Art. 24.** Esta instrução normativa entra em vigor na data da sua publicação.

Publique-se

Recife, 19 de julho 2024.

**Des. Ricardo Paes Barreto**

**Presidente do Tribunal de Justiça de Pernambuco**

PODER JUDICIÁRIO

**TRIBUNAL DE JUSTIÇA DE PERNAMBUCO**

**INSTRUÇÃO NORMATIVA Nº 31, DE 19 DE JULHO DE 2024**

EMENTA: Institui, no âmbito do Poder Judiciário de Pernambuco, o Protocolo de Investigação de Ilícitos Cibernéticos (PIIC).

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA DE PERNAMBUCO** , Desembargador Ricardo Paes Barreto, no uso de suas atribuições legais e regimentais, e

**CONSIDERANDO** a necessidade de adotar e seguir o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, consoante o disposto no art. 26 da Resolução CNJ nº 396, de 07 de junho de 2021;

**CONSIDERANDO** a necessidade de implementar o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, conforme art. 5º da Portaria CNJ nº 162, de 10 de junho de 2021, levando em conta as peculiaridades do Tribunal de Justiça de Pernambuco;

**CONSIDERANDO** a característica de complementariedade e a necessidade de harmonização entre os Protocolos de Gerenciamento de Crises Cibernéticas, de Prevenção de Incidentes Cibernéticos e de Investigação de Ilícitos Cibernéticos do Poder Judiciário, todos aprovados pela Portaria CNJ nº 162, de 10 de junho de 2021;

**CONSIDERANDO** o cenário mundial de aumento nos crimes cibernéticos, inclusive tendo como alvo instituições públicas;

**CONSIDERANDO** a necessidade urgente de aprimoramento dos instrumentos de governança e gestão de segurança da informação que permeiam todos os níveis da Instituição.

**RESOLVE** :

## CAPÍTULO I

## DAS DISPOSIÇÕES PRELIMINARES

**Art. 1º** Instituir, no âmbito do Poder Judiciário de Pernambuco, o Protocolo de Investigação de Ilícitos Cibernéticos (PIIC).

**Art. 2º** O PIIC tem como objetivo estabelecer procedimentos para garantir a existência, a qualidade, a coleta e a preservação de evidências, bem como para a comunicação aos órgãos competentes para início da persecução penal.

## CAPÍTULO II

## DA ADEQUAÇÃO DOS ATIVOS TECNOLÓGICOS

**Art. 3º** Compete à Secretaria de Tecnologia da Informação e Comunicação (SETIC) manter data, hora e fuso horário dos ativos de TIC (equipamentos e sistemas) automaticamente sincronizados com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional.

**Art. 4º** Compete ainda à SETIC configurar os ativos de TIC para registrar logs de todos os eventos relevantes, considerando, mas não se limitando aos seguintes tipos de eventos:

**I** – autenticações bem e malsucedidas;

**II** – acessos autorizados e não autorizados aos recursos e dados privilegiados;

**III** – acessos e alterações em registros de auditoria.

**Art. 5º** Os *logs* mencionados no art. 4º devem incluir necessariamente:

**I** – data, hora e fuso horário sincronizados;

**II** – identificação inequívoca do usuário;

**III** – descrição da natureza do evento;

**IV** – endereços de internet (IPs), nome de rede do ativo ou outros identificadores, se existirem;

**V** – endereços de internet (IPs) e portas de origem e de destino em casos de evento envolvendo conexões de rede;

VI – coordenada geográfica ou outro tipo indicativo de localização geográfica do instante do evento, se houver; e

**VII** – quaisquer outras informações que possam identificar a origem e a causa do evento no contexto cujo ativo de TIC está inserido.

**Art. 6º** Os ativos de informação que não propiciem os registros dos eventos listados no art. 5º serão mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

**Art. 7º** As redes de comunicação e os sistemas serão monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

**I** – utilização de usuários, perfis e grupos privilegiados;

**II** – modificações da lista de membros de grupos privilegiados;

**III** – utilizações, criações, alterações e exclusões de credenciais administrativas e elevações de credenciais para funções administrativas, em especial para administradores de domínio de rede e administradores de mais alto nível em sistemas;

**IV** – inicialização, suspensão e reinicialização de serviços;

**V** – acoplamento, operações (cópia, alteração, movimentação, etc.) sobre conteúdos e desacoplamento de dispositivos de *hardware* , com especial atenção para mídias removíveis;

**VI** – modificações de política de senhas, como, por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, etc.;

**VII** – acesso ou modificação de arquivos ou sistemas considerados críticos; e

**VIII** – eventos obtidos por meio de quaisquer mecanismos de segurança existentes.

**Art. 8º** A retenção padrão de todos dos registros de eventos em *logs* de que trata esta Instrução Normativa será de, no mínimo, 06 (seis) meses, sem prejuízo de prazos maiores previstos em outros normativos.

**Parágrafo único.** A priorização para guarda dos *logs* levará em conta a disponibilidade de recursos para este fim, buscando-se meios de atender aos prazos de retenção, dispostos neste protocolo, e tendo em vista a criticidade do ativo em função da sua relação com os sistemas considerados mais críticos para as áreas de negócio de acordo com as orientações mais recentes do Conselho Nacional de Justiça (CNJ).

**Art. 9º** Cada integrante da Equipe de Tratamento e Respostas a Incidentes do TJPE (ETIR) deve estar ciente de todos os dispositivos deste Protocolo e reportar, preventivamente à SETIC, eventuais fatores que impliquem a impossibilidade de atendimento ao Protocolo no caso do seu acionamento.

## CAPÍTULO III

## DA PRESERVAÇÃO DE EVIDÊNCIAS

**Art. 10** A coleta de evidências em incidentes penalmente relevantes é de responsabilidade da ETIR, sob supervisão de seu (sua) agente responsável, e compreende, no mínimo, coletar e preservar:

**I** – mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;

**II** – dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e

**III** – todos os registros de eventos citados neste Protocolo.

**Art. 11** . As ações de restabelecimento do serviço, para níveis parciais ou normais de operação, priorizarão o não comprometimento da coleta e da integridade das evidências, e considerarão todos os cuidados com a cadeia de custódia dispostos neste protocolo.

**Parágrafo único.** Nos casos em que a necessidade de pronto restabelecimento do serviço implique, necessariamente, a inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, deve-se adotar os seguintes procedimentos:

**I** – as inviabilidades devem ser comunicadas pela ETIR ao Comitê Gestor de Crises e à Presidência;

**II** – o Comitê Gestor de Crises ou Presidência deliberará sobre a coleta ou não das evidências, considerando os impactos, e informará formalmente à ETIR sobre a decisão;

**III** – a ETIR, sob a supervisão do(a) seu(sua) responsável, coletará e armazenará cópia dos arquivos afetados pelo incidente, tais como logs, configurações de sistema operacional, arquivos de sistemas de informação e outros julgados necessários, mantendo-se a estrutura de diretórios original e os “metadados” desses arquivos, como data, hora de criação, fuso horário e permissões; e

**IV** – o(a) agente responsável pela ETIR fará constar de relatório formal a impossibilidade de preservação das mídias afetadas e listará todos os procedimentos adotados.

**Art. 12.** Em qualquer caso de coleta de arquivos, inclusive dos arquivos referidos no art. 10, para a preservação das evidências, deve-se:

**I** – gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados;

**II** – gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos no inciso I deste artigo; e

**III** – gerar e gravar resumo criptográfico do arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados a que se refere o inciso I deste artigo.

**Art. 13.** Todo material coletado deverá ser lacrado e custodiado pelo(a) agente responsável pela ETIR, que preencherá Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante.

**Art. 14.** O material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.

## CAPÍTULO IV

**DA COMUNICAÇÃO DO INCIDENTE**

**Art. 15.** O incidente penalmente relevante deve ser informado imediatamente ao Comitê de Governança da Segurança da Informação (CGSI), à Presidência e ao Comitê de Crise de Segurança Cibernética.

**Art. 16.** A Presidência, o(a) Coordenador(a) do CGSI ou o(a) Diretor(a) Geral comunicará o incidente penalmente relevante de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos e ao Ministério Público.

**Art. 17.** Cabe ao Comitê de Crise de Segurança Cibernética avaliar se o incidente informado se caracteriza como uma crise, fundamentado nos critérios estabelecidos no Protocolo de Gerenciamento de Crises Cibernéticas.

**Art. 18.** Findados os procedimentos de coleta e preservação de evidências do incidente penalmente relevante cabe ao(à) agente responsável pela ETIR elaborar o Relatório de Comunicação de Incidente de Segurança Cibernética.

**Art. 19.** O Relatório de Comunicação de Incidente de Segurança Cibernética deve conter, no mínimo, as seguintes informações, sem prejuízo de outras consideradas relevantes:

**I** – nome do(a) responsável pela preservação dos dados do incidente, com informações de contato;

**II** – nome do(a) agente responsável pela ETIR e informações de contato;

**III** – órgão comunicante com sua localização e informações de contato;

**IV** – número de controle da ocorrência no formato sequencial-ano;

**V** – relato descrevendo o ocorrido, como foi detectado e quais dados foram coletados e preservados;

**VI** – descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;

**VII** – resumo criptográfico dos arquivos coletados;

**VIII** – termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

**IX** – número de lacre de material físico preservado, se houver; e

**X** – justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados.

**§1º** O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais será emitido em três vias (cópias) e cada uma deve ser acondicionada em envelope lacrado e rubricado pelo(a) agente responsável pela ETIR, protocolado e encaminhado formalmente à Presidência, ao(à) Coordenador(a) do CGSI ou ao(à) Diretora Geral.

**§2º** O envelope lacrado deve conter em sua capa, além de informações do órgão remetente e do órgão destinatário, descrição de que se trata de comunicação de evento relacionado à segurança da informação, sem qualquer detalhamento sobre os fatos.

**Art. 20.** Recebida a Comunicação de Incidente de Segurança em Redes Computacionais, a Presidência, o(a) Coordenador do CGSI ou o(a) Diretor(a) Geral deverá:

**I** – arquivar uma das cópias; e

**II** – encaminhar formalmente as demais cópias lacradas ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com o todo o material previsto neste protocolo, para fins de instrução da notícia crime.

**Art. 21.** Esta Instrução Normativa entra em vigor na data da sua publicação.

Publique-se

Recife, 19 de julho 2024.

**Des. Ricardo Paes Barreto**

**Presidente do Tribunal de Justiça de Pernambuco**

PODER JUDICIÁRIO

**TRIBUNAL DE JUSTIÇA DE PERNAMBUCO**

**INSTRUÇÃO NORMATIVA Nº 32, DE 19 DE JULHO DE 2024**