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

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

EMENTA: Institui, no âmbito do Poder Judiciário de Pernambuco, o Protocolo de Prevenção de Incidentes Cibernéticos (PPIC/PJPE).

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 Prevenção de Incidentes Cibernéticos (PPIC/PJPE).

Art. 2º O PPIC/PJPE é fundamentado em princípios críticos de prevenção aos incidentes cibernéticos que são compostos por funções que viabilizam a gestão institucional de riscos de segurança da informação.

Art. 3º A gestão institucional de riscos de segurança da informação dará suporte adequado à mitigação ou aceitação de riscos, sempre em alinhamento com a segurança da informação e as necessidades de prestação jurisdicional do Poder Judiciário de Pernambuco (PJPE).

CAPÍTULO II

DOS PRINCÍPIOS CRÍTICOS

Art. 4º São princípios críticos de prevenção no âmbito do PJPE:

I – base de conhecimento e defesa: buscar a utilização de todo e qualquer recurso viável que disponibilize histórico, catálogos com modelos de referência, bases estruturadas, redes de colaboração do Poder Judiciário, descrições, análises e pesquisas elaboradas por outras entidades, etc., cujo tema sejam ataques reais que tenham comprometido ou vulnerabilidades que possam viabilizar um eventual comprometimento de ambientes tecnológicos;

II – priorização: priorizar a segurança da informação dentro do PJPE tanto no que tange a pessoas, processos e tecnologias mantidos pela Secretaria de Tecnologia da Informação (SETIC), quanto no que se refere a magistrados(as) e servidores(as) de todas as áreas e níveis, com foco no provisionamento de tecnologia segura, de conscientização e treinamento, no refinamento da segurança do provisionamento de acessos como um todo e na implementação de processos seguros.

III – instrumentos de medição e métricas: implementar e manter a capacidade de medir e tornar compreensível para os setores envolvidos o estado da segurança da informação do PJPE, incluindo medidas como as de avaliar a propensão dos usuários a cair em estratégias de engenharia social advindas dos mais diversos meios, acompanhar a evolução da aplicação de correções de segurança no ambiente, quantificar as tentativas de ataque detectadas nas ferramentas existentes, quantificar sistemas que possuem e os que não possuem medidas satisfatórias de autenticação segura, dentre outras.

IV – diagnóstico contínuo: utilizar meios para identificar continuamente, de forma automática ou manual, a eficácia dos controles tecnológicos ou administrativos de segurança aplicados são eficazes, incluindo medidas como as de reavaliação de termos e contrato pela área jurídica do TJPE, reavaliação de tecnologias de segurança mediante comparação com tecnologias mais recentes, revisão de segurança nas implementações em infraestruturas físicas, ambientes lógicos, códigos fontes e executáveis, avaliação constante e ampla de pessoas das mais diversas áreas do TJPE, dentre outros.

V – formação, capacitação e conscientização: planejar, implementar e executar ações formais de educação continuada, para fins de consolidar cultura de segurança da informação robusta dentro do PJPE.

VI – automação: priorizar a utilização de soluções automatizadas para os mais diversos fins (ex.: incidentes, treinamento, gestão de riscos de segurança da informação, inventário de ativos e dados, conscientização, etc.) dentro da área de segurança da informação.

VII – resiliência: prever, desde a concepção, a utilização de recursos e estratégias que viabilizem sempre a maior robustez na resistência e na recuperação em caso de incidentes, mediante utilização de ferramentas tecnológicas, recursos relacionados aos fluxos e processos, planos de recuperação, contingências e pessoas treinadas e conscientes.

Parágrafo único. Os princípios críticos, dispostos neste artigo, devem ser aplicados pelos meios e na proporção que forem viáveis e necessários, preferencialmente balizados por avaliações formais de gestão de riscos de segurança da informação.

CAPÍTULO III

DAS FUNÇÕES BÁSICAS

Art. 5º As funções básicas e ações mínimas da prevenção, no âmbito do PJPE, serão implementadas pelos seguintes responsáveis:

I – identificação:

a) mapeamento dos processos de negócio e levantamento dos sistemas considerados críticos de acordo com as orientações mais recentes do Conselho Nacional de Justiça (CNJ): Secretaria de Planejamento (SEPLAN);

b) divulgação formal dos processos de negócio e sistemas críticos: Presidência do TJPE;

c) identificação e inventário de ativos tecnológicos (hardware e software) que suportam os sistemas críticos identificados na alínea “a”: Secretaria de Tecnologia da Informação e Comunicação (SETIC);

d) identificação e listagem de magistrados(as), servidores(as) e quaisquer outros(as) usuários(as) em sistemas para fins de treinamento e conscientização em segurança, medidas preventivas e tomadas de decisões: Secretaria de Tecnologia da Informação e Comunicação (SETIC);

e) indicação de necessidade de privilégios de acessos e forma de acesso (presencial ou remota) de usuários(as) de processos de negócio e sistemas críticos: áreas de negócio do TJPE responsáveis pelos processos de negócio e sistemas críticos;

f) quantificação de riscos de segurança da informação que envolvem os ativos de suporte de processos de negócio e sistemas críticos: Secretaria de Tecnologia da Informação e Comunicação (SETIC);

g) avaliação e tomada dè decisões quanto à mitigação e aceitação de riscos de segurança da informação: Presidência do TJPE, Comitê de Governança da Segurança da Informação (CGSI), Comitê Gestor de Proteção de Dados (CGPD), Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC), Comitê Gestor de Crise Cibernética (CGCC), qualquer área de negócio do TJPE com interesse relevante no processo ou sistema ou Secretaria de Tecnologia da Informação e Comunicação (SETIC), a depender da relevância, impacto e probabilidade do cenário de risco em questão;

II – proteção:

a) elaboração de planos de tratamento de riscos de segurança da informação no que tange aos ativos tecnológicos: Secretaria de Tecnologia da Informação e Comunicação (SETIC);

b) planejamento, implementação, manutenção ou contratação, em forma de serviços ou produtos, de controles tecnológicos de segurança da informação, com base nos planos de tratamento mencionados na “alínea a” ou por iniciativas independentes dos planos: Secretaria de Tecnologia da Informação e Comunicação (SETIC);

c) implementação e manutenção de controles de segurança da informação em processos de negócio: qualquer área de negócio do TJPE com interesse ou participação no processo;

d) planejamento, desenvolvimento e execução de ações formais de educação em segurança da informação, aproveitáveis, quando viável, para fins de progressão funcional considerando as regras vigentes (ações a serem consideradas nas análises de planejamento: programas de formação; programas de reciclagem; programas de extensão educacional; programas de pesquisa e fomento de natureza técnica, acadêmica e científica; elaboração de artigos, materiais e publicações de natureza técnica, acadêmica e científica; programas de intercâmbio, imersão e cooperação educacional; ações periódicas de capacitação; cursos em plataformas do tipo MOOC – Massive Open On-line Courses; cursos em plataformas alternativas especializadas em segurança da informação contratadas pelo TJPE; programas de certificação especializada; palestras, congressos, seminários e afins; concursos, competições e premiações; e workshops): Escola Judicial de Pernambuco (ESMAPE) e Secretaria de Gestão de Pessoas (SGP);

e) estabelecimento de carga horária mínima de capacitação em segurança da informação a serem cumpridas por magistrados(as) e servidores(as), em proporções que se entenderem adequadas nas seguintes modalidades: ações de capacitação em geral; cursos de educação executiva de curta duração; cursos de graduação; cursos de especialização; cursos de mestrado; cursos de doutorado; e cursos de pós-doutorado: Presidência do TJPE, Escola Judicial de Pernambuco (ESMAPE) e Secretaria de Gestão de Pessoas (SGP).

f) planejamento, desenvolvimento e execução de ações de conscientização de difusão com amplo alcance, tais como: campanhas; produção de panfletos, cartazes, folhetos, notas informativas e/ou boletins periódicos; e testes públicos de segurança: Assessoria de Comunicação do TJPE (ASCOM), Escola Judicial de Pernambuco (ESMAPE) e Secretaria de Tecnologia da Informação e Comunicação (SETIC).

III – detecção (monitoramento, testes, etc.):

a) monitoramento contínuo, 24 horas por dia e 7 dias por semana, por meios próprios ou por terceiro contratado, do ambiente tecnológico do PJPE com o intuito de evidenciar, o mais precocemente possível, eventos e incidentes relacionados à segurança da informação, considerando as funções, reconhecidas como boas práticas em segurança, de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas: Secretaria de Tecnologia da Informação e Comunicação (SETIC).

b) análise, teste, identificação e quantificação, por meios próprios ou por terceiro contratado, do ambiente tecnológico do PJPE com o intuito de evidenciar, o mais precocemente possível, vulnerabilidades em ativos, procedimentos e pessoas relacionadas à segurança da informação: Secretaria de Tecnologia da Informação e Comunicação (SETIC).

IV – resposta:

a) elaboração de documentação necessária de procedimentos técnicos para resposta imediata em situações de incidente de segurança da informação, considerando as funções, reconhecidas como boas práticas em segurança, de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas: Secretaria de Tecnologia da Informação e Comunicação (SETIC).

V – recuperação:

a) elaboração de Planos de Recuperação de Desastre de TIC para cenários de crise considerando a criticidade dos ambientes e riscos que os envolvem: Secretaria de Tecnologia da Informação e Comunicação (SETIC).

b) elaboração de Planos de Continuidade de Negócio para cenários de crise que envolvam comprometimentos parcial ou total de ambientes de tecnologia da informação: Secretaria de Planejamento (SEPLAN).

Art. 6º Detalhamentos sobre desdobramentos decorrentes do disposto nesta instrução normativa, caso necessários, devem ser buscados nas normas internas do PJPE, nas normas vigentes aplicáveis a todo o Poder Judiciário, nas legislações nacionais vigentes e nas normas técnicas de referência publicadas por órgãos de normatização técnica sobre boas práticas de segurança da informação e continuidade de negócios.

CAPÍTULO IV

DA EQUIPE DE TRATAMENTO E RESPOSTA A

INCIDENTES DE SEGURANÇA CIBERNÉTICA

Art. 7º O Tribunal de Justiça de Pernambuco constituirá Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), contemplando os requisitos dispostos nas normas atuais publicadas pelo Conselho Nacional de Justiça (CNJ) aplicáveis aos Órgãos do Judiciário.

Parágrafo único. A ETIR poderá estender e ampliar a operação de suas funções, nos termos das normas vigentes, por meio de servidores(as) efetivos e de contratos de ferramentas e serviços prestados por terceiros.

Art. 8º 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

PORTARIA N° 62, DE 19 DE JULHO DE 2024

Altera a Portaria nº 10/2024, publicada no DJe do dia 12/03/2024, que dispõe sobre a criação da Comissão Examinadora do Concurso Público para Provimento de Cargo de Juiz Substituto de 1ª Entrância da Carreira da Magistratura do Estado de Pernambuco e dá outras providências.

O Presidente do Tribunal de Justiça do Estado de Pernambuco, Exmo. Des. Ricardo Paes Barreto, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o disposto no art. 30, inciso XIV, do Regimento Interno do Tribunal de Justiça do Estado de Pernambuco (Resolução TJPE nº 395, de 29.03.2017);

CONSIDERANDO o disposto na Lei Complementar nº 472, de 27 de dezembro de 2021, que alterou a a Lei Complementar Estadual nº 100, de 21 de novembro de 2007 - Código de Organização Judiciária do Estado de Pernambuco, para adequar a composição da Comissão do Concurso para provimento do cargo de Juiz Substituto de 1ª Entrância da Magistratura do Estado de Pernambuco aos termos da Recomendação do Conselho Nacional de Justiça n° 85, de 12 de janeiro de 2021 e da Resolução Conjunta CNJ/CNMP n° 07, de 25 de junho de 2021,

RESOLVE: