Kathleen Nicola Kilian	Carla Cristine de Souza Pires	Vara Única da Comarca de Cariré Vara Única da Comarca de Coreaú Vara Única da Comarca de Mauriti 1ª Vara da Comarca de Mombaça
	Clara Moreira Carvalho	
	Larissa Sousa Mendes	
	Monaliza Canuto Rodrigues Bezerra	
Luiz Eduardo Viana Pequeno	Ney Franklin Fonseca de Aquino	Vara Única da Comarca de Amontada Vara Única da Comarca de Capistrano 17ª Unidade do Juizado Especial Cível da Comarca de Fortaleza Vara Única da Comarca de Irauçuba Vara Única da Comarca de Reriutaba Vara Única da Comarca de Uruoca
	Renata Martins Dias Dávila	
	Ricardo Barbosa Silva	
	Rodolfo da Rocha Melo	
Patrícia Fernanda Toledo Rodrigues	Carla Tais Dourado Silva Vasconcelos	1ª Vara da Comarca de Camocim Vara Única da Comarca de Ipaumirim Vara Única da Comarca de Santana do Acaraú
	Eduardo Augusto Ferreira Abreu Filho	
	Francisca Narjana de Almeida Brasil	
	Quéren Bandeira Mesquita de Albuquerque	
Paulo Sérgio Reis	Amanda Monte Lima	2ª Vara Cível da Comarca de Santa Quitéria 1ª Vara da Comarca de Massapê 1ª Vara da Comarca de Horizonte Juizado Especial Cível e Criminal da Comarca de Sobral Vara Única da Comarca de Solonópole Vara Única da Comarca de Chaval
	André Medeiros Sales	
	Renata Valéria Lima Leitão	
	Wanine Marcelle Dias	

§1º. Aos(as) juízes(juízas) leigos(as) designados(as) na forma do caput deste artigo competirão o desempenho das funções constantes no §1º do art. 1º da Resolução nº 02/2019 do Órgão Especial do TJCE.

Art. 3º A Secretaria de Tecnologia da Informação deverá providenciar os acessos necessários aos fluxos dos sistemas processuais utilizados nas unidades em referência.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

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

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA, aos 28 dias do mês de novembro de 2022.

DESEMBARGADOR MARIA NAILDE PINHEIRO NOGUEIRA
PRESIDENTE DO TRIBUNAL DE JUSTIÇA

PORTARIA Nº 2521/2022

Dispõe sobre os protocolos de prevenção de incidentes, gerenciamento e investigação de ilícitos cibernéticos no Poder Judiciário do Estado do Ceará.

A PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ (TJCE), no uso das atribuições legais e regimentais,

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

CONSIDERANDO os termos da Portaria do CNJ n° 162, que aprovou protocolos e manuais criados pela Resolução CNJ n° 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO os termos da Resolução do Órgão Especial n° 07/2022, que atribui ao Comitê de Governança de Segurança Informação e de Crises Cibernéticas a Elaboração da Política de segurança da Informação e normas internas correlatas;

CONSIDERANDO as boas práticas de Governança de Segurança e Tecnologia da Informação que visam a garantir a disponibilidade e a integridade de sistemas, aplicativos, dados e documentos digitais do Poder Judiciário do Estado do Ceará;

RESOLVE:

Art. 1º Aprovar os Anexos I, II e III, desta Portaria, que contêm, respectivamente, os seguintes protocolos:
I - Prevenção de Incidentes Cibernéticos do Poder Judiciário do Estado do Ceará (PPINC-PJCE);
II - Gerenciamento de Crises Cibernéticas do Poder Judiciário do Estado do Ceará (PGCC-PJCE); e
III - Investigação para Ilícitos Cibernéticos do Poder Judiciário do Estado do Ceará (PIIC-PJCE).

Art. 2º Esta Portaria entra em vigor na da sua publicação.

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

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, em Fortaleza, aos 29 de novembro de 2022.

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

ANEXO I DA PORTARIA Nº 2521/2022

PROTOCOLO DE PREVENÇÃO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO DO ESTADO DO CEARÁ

(PPINC-PJCE)

Art. 1º O **Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário do Estado do Ceará (PPINC-PJCE)** contempla um conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível.

Art. 2º Este protocolo é composto por: funções básicas que expressem a gestão do risco organizacional e que permitam as decisões adequadas para o enfrentamento de ameaças e a melhor gestão de práticas e de metodologias existentes; conceitos, boas práticas de segurança cibernética; gestão de incidentes de segurança da informação; processo e plano de gestão de incidente de segurança da Informação; e é complementado pelos protocolos de Gerenciamento de Crises Cibernéticas de Investigação para Ilícitos Cibernéticos do Poder Judiciário do Estado do Ceará.

Art. 3º São funções básicas do PPINC-PJCE: identificar, proteger, detectar, responder e recuperar, nos seguintes termos:

I - identificar: entendimento organizacional para gerenciar o risco direto e/ou indireto de ataques cibernéticos a sistemas, pessoas, ativos, dados e recursos. Permite ao TJCE avaliar os recursos que suportam funções críticas e os riscos relacionados. São medidas de concentração e priorização dos esforços na gestão de ativos, ambiente de negócios, governança, avaliação de riscos e estratégia de gestão de riscos;

II - proteger: desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, e de ativos de informação, bem como a prestação de serviços críticos;

III - detectar: desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de segurança cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de detecção de anomalias e eventos;

IV - responder: desenvolvimento e implementação de atividades apropriadas à adoção de medidas em incidentes cibernéticos detectados. Nessa categoria, são incluídos os planos de resposta, de comunicações, de análise, de mitigação e de melhorias; e

V - recuperar: desenvolvimento, implementação e manutenção dos planos de resiliência e de restauração de quaisquer capacidades ou serviços que foram prejudicados em razão de incidentes de segurança cibernética.

Art. 4º Para efeito deste protocolo consideram-se:

I - base de conhecimento: consiste no uso de informações e conhecimento de ataques reais que comprometeram sistemas. Informações conseguidas por meio de experiências vivenciadas pelas equipes técnicas e interação e de cooperação com outras equipes de tratamento a incidentes e respostas;

II - priorização: foco prioritário na formação, na revisão de controles/acessos, nos processos e na disseminação da cultura de segurança cibernética. Contribui para a redução de riscos e para a proteção contra as ameaças mais sensíveis e que encontram viabilidade em sua célere implementação;

III - instrumentos de medição e métricas: definição e estabelecimento de métricas comuns que fornecem linguagem compartilhada e de compreensão abrangente para magistrados, servidores, colaboradores, prestadores de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança. Permite a medição da eficácia das medidas de segurança dentro do TJCE. Fornece insumos para que os ajustes necessários, quando identificados, possam ser implementados de forma célere;

IV - diagnóstico contínuo: processo de trabalho que realiza continuamente medição para testar e validar a eficácia das medidas de segurança atuais e contribui para a definição de prioridades e para os próximos passos a serem tomados;

V - formação, capacitação e conscientização: processos formais de educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação, a conscientização e a instrução para todos os atores envolvidos em atividades diretas ou indiretas que contribuam para a cultura de segurança cibernética dentro da organização. Tais instrumentos deverão ser revisados periodicamente;

VI - automação: incentivo à busca de soluções automatizadas de segurança cibernética para que as organizações obtenham medições confiáveis, escaláveis e contínuas; e

VII - resiliência: poder de recuperação ou capacidade de a organização resistir aos efeitos de um incidente, bem como impedir a reincidência secundária do incidente identificado.

Art. 5º Compete as áreas abaixo descritas as seguintes atribuições na Gestão de Incidentes de Segurança Cibernética devem ser observadas:

I - equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR):

a) deverá ser formalmente instituída Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR);

b) a ETIR poderá solicitar apoio multidisciplinar para responder aos incidentes de segurança de maneira adequada e tempestiva, em áreas como: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras;

c) o Comitê de Governança de Segurança da Informação (CGSICC) avaliará o adequado posicionamento da ETIR no organograma institucional, considerando-se o desenho organizacional e suas peculiaridades;

d) a ETIR terá autonomia compartilhada, ou seja, participará do resultado da decisão recomendando 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; e

e) o funcionamento da ETIR deverá ser regulado por documento formal de constituição, publicado no sítio eletrônico do TJCE, devendo constar, no mínimo, os seguintes pontos: definição da missão, público-alvo, modelo de implementação, nível de autonomia, designação de integrantes, canal de comunicação de incidentes de segurança e serviços que serão prestados.

II - Comitê de Gestão de Tecnologia da Informação e Comunicação – CGETIC:

a) contactar atores externos, aguardar informações/aprovação, reunir-se durante crises cibernéticas para apoiar o Comitê de Crises.

III - Grupos Resolvedores:

a) realizar ações de contenção.

IV - Supervisão da Área de Segurança da Informação:

a) realizar com o apoio da ETIR e outras áreas a gestão do incidente cibernético.

Art. 6º O Presente protocolo deverá observar as seguintes práticas:

I - a segurança cibernética é um empreendimento coletivo. Para melhor detectar, conter e eliminar ataques cibernéticos

e minimizar eventuais impactos na operação, assegurando o funcionamento dos sistemas críticos do TJCE, sobretudo em ambiente de constante ameaça, é necessário possuir mecanismos de respostas e prevenção.

II - a prevenção a incidentes contempla funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

III - São assim definidas as dimensões e práticas da segurança cibernética:

a) preparação: processo que envolve as equipes de tratamento a incidentes e respostas. Trata-se de resposta metódica, contemplando ferramentas forenses de análise e custódia, planejamento sobre como responder e notificar cada incidente de segurança, identificação de cadeia de comando em situação de crise, processos de educação e de formação;

b) identificação: capacidade de identificar que um ataque cibernético está em andamento, por meio da percepção de sinais de anomalias ou de comportamentos inesperados. Trata-se da aptidão dos entes para diferenciar as irregularidades em redes de dados e identificar o mau funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso. Para essa atividade, podem ser elaboradas listas de verificação investigativas para apoiar o processo de diagnóstico, triagem e acionamento das equipes de resposta, permitindo a avaliação do impacto e a determinação dos próximos passos a serem tomados;

c) contenção: visa a garantir que o incidente não cause mais danos. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa incluindo, dentre outros, a imediata comunicação prevista na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSECPJ) e seus anexos, o isolamento da fonte do ataque, a aplicação de ferramentas forenses para remoção de malware das redes de produção, a limitação de transferências de dados desnecessárias e a adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises Cibernéticas;

d) erradicação: remoção da ameaça, garantindo que as operações essenciais sejam apoiadas, caso surjam desafios no processo de restauração. Os métodos possíveis para essa função podem variar desde patches ou reconstruções do sistema até redesenho completo da arquitetura, devendo, sempre que possível, preservar evidências que apoiarão o processo de investigação do crime cibernético;

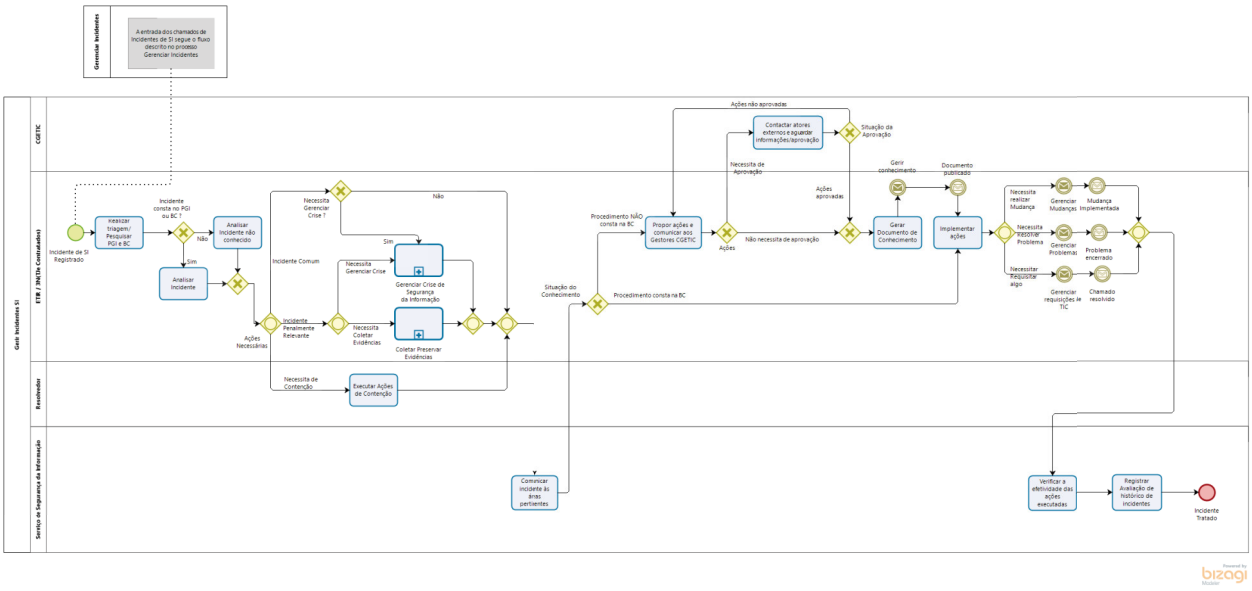
e) recuperação: promulgação de plano de recuperação em fases para restauração de operações, com foco prioritário nos sistemas críticos ou na execução da operação em modo analógico até que haja confiança no desempenho do sistema. Nessa atividade, são necessárias verificações ambientais e de segurança paralelas ao controle dos impactos de desempenho não intencionais da restauração;

f) lições aprendidas: atividade contínua que não só deve capturar os impactos imediatos de um incidente, mas também as melhorias em longo prazo da segurança cibernética do órgão. Tal função pode variar de um sistema de controle de processos melhor projetado até a evolução e preparação de centros de identificação e resposta a ataques cibernéticos do Poder Judiciário.

Art. 7º O presente protocolo deverá observar o Plano de Gestão de Incidentes de Segurança da Informação:

I - o plano tem o objetivo de estabelecer princípios, conceitos, diretrizes e responsabilidades nas fases de detecção, resolução, prevenção e redução da ocorrência sobre a gestão de incidentes de segurança da informação no TJCE, orientando o funcionamento do processo, de forma que este seja tratado adequadamente, mitigando ao máximo os impactos para o negócio, proporcionando um ambiente cada vez mais confiável, disponível e íntegro; e

II - a gestão de incidentes de segurança cibernética é realizada por meio de processo (fluxo) abaixo:



O Plano de Gestão de Incidente de Segurança da Informação pode ser acessado pelo link: https://tjnet/wp-content/uploads/2022/08/plano-de-gestao-de-incidentes-de-si-versao-final.pdf

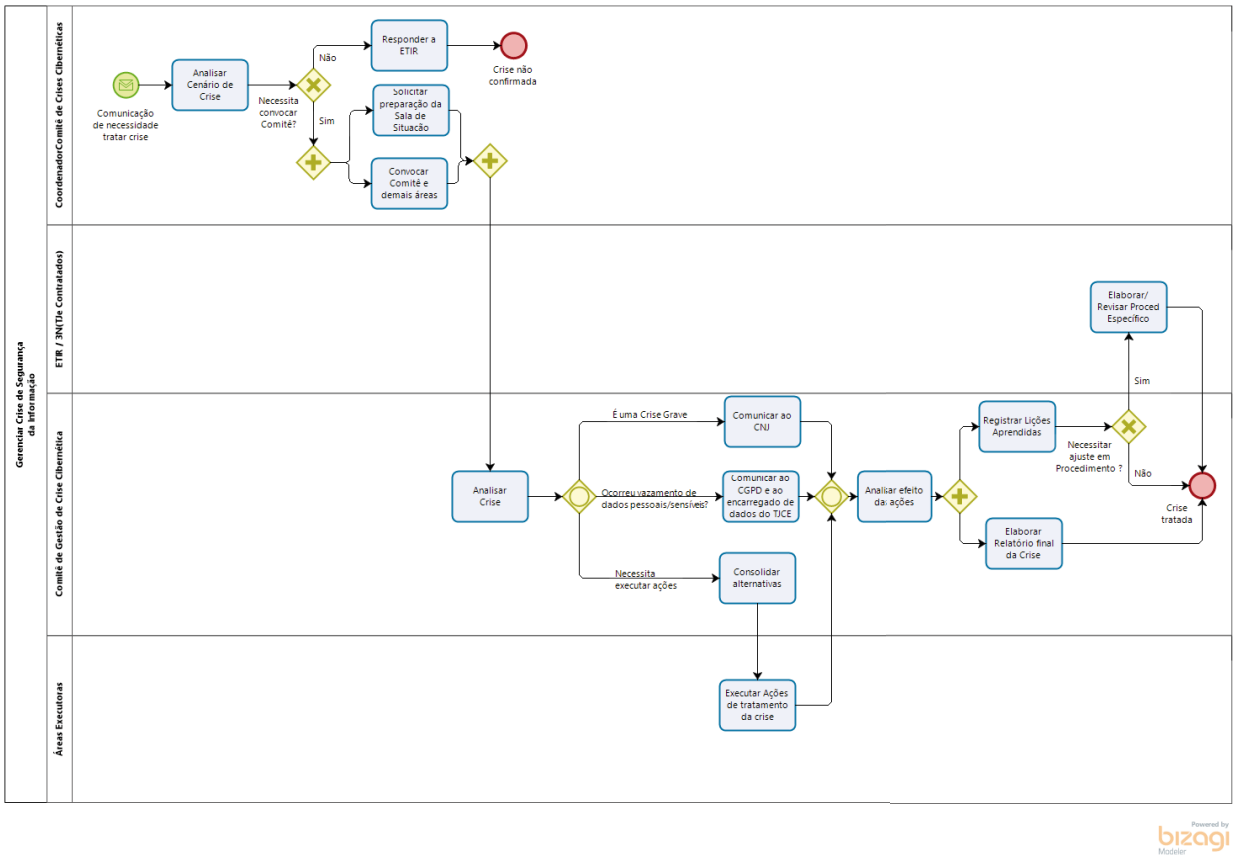
ANEXO II DA PORTARIA Nº 2521/2022

PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS DO PODER JUDICIÁRIO DO ESTADO DO CEARÁ (PGCC-PJCE)

Art. 1º O Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário do Estado do Ceará é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos do Estado do Ceará e prevê as ações responsivas a serem colocadas

em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses. Fazem parte deste protocolo os itens: o processo Gerenciar Crise de Segurança da Informação, identificação de crise cibernética, as fases do gerenciamento de crises, o planejamento da Crise (pré-crise), execução (durante a crise), melhoria contínua e lições aprendidas no pós-crise.

Art. 2º Processo Gerenciar Crise de Segurança da Informação:



Art. 3º Identificação de Crise Cibernética:

Parágrafo único. O gerenciamento de incidentes se refere às atividades que devem ser executadas para avaliar o problema e determinar a resposta inicial diante da ocorrência de um evento adverso de segurança da informação.

I - o gerenciamento de crise se inicia quando:

a) ficar caracterizado grave dano material ou de imagem;

b) restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

c) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou

d) o incidente atrair grande atenção da mídia e da população em geral.

Art. 4º Fases do Gerenciamento de Crises:

Parágrafo único. O Gerenciamento de Crises pode ser dividido em 3 (três) fases:

I - planejamento (pré-crise);

II - execução (durante a crise); e

III - melhoria Contínua (pós-crise).

Art. 5º Planejamento da Crise (pré-crise):

I - Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que o TJCE estabeleça um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:

a) observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário do Estado do Ceará;

b) definir as atividades críticas que são fundamentais para a atividade finalística do Poder Judiciário do Estado do Ceará;

c) identificar os ativos de informação críticos, ou seja, aqueles que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;

d) avaliar continuamente os riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;

e) categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos;

f) priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade. Tais atividades deverão ser detalhadas e consolidadas em um plano de contingência que contemple diversos setores, em razão de possíveis cenários de crise, a fim de se contrapor à escalada de uma eventual crise e com o objetivo de manter os serviços prestados pela organização; e

g) realizar simulações e testes para validação dos planos e procedimentos.

II - Deve-se definir a sala de situação e criar um Comitê de Crises Cibernéticas, composto por representantes da alta

administração e por representantes executivos, com suporte da ETIR e de especialistas:

a) da área Jurídica;
b) da área de Comunicação Institucional;
c) da área de Tecnologia da Informação e Comunicação;
d) da área de Privacidade de Dados Pessoais;
e) da área de Segurança da Informação;
f) das unidades administrativas de apoio à contratação; e
g) da área de Segurança Institucional.

Art. 6° Execução (durante a crise):

I - assim que a ETIR ou o CGETIC identificar que um incidente constitui uma crise cibernética, o Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC) deverá se reunir imediatamente na sala de situação previamente definida;

II - os planos de contingência existentes, caso, aplicáveis, devem ser efetivados imediatamente, visando à continuidade dos serviços prestados;

III - a coordenação do CGSICC deve ficar a cargo de indicado pelo (a) Presidente do do Poder Judiciário do Estado do Ceará, com autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações;

IV - a sala de situação é o local a partir do qual serão geridas as situações de crise, devendo dispor dos meios necessários (ex.: sistemas de áudio, vídeo, chamadas telefônicas) e estar preferencialmente próxima a um local onde se possa fazer declarações públicas à imprensa e com acesso restrito ao CGSICC e a outros entes eventualmente convidados a participar das reuniões;

V - a sala de situação deve ser um ambiente que permita ao Comitê deliberar com tranquilidade e que possua uma equipe dedicada à execução de atividades administrativas para o período da crise;

VI - para eficácia do trabalho, é necessário o CGSICC:

a) entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;
b) levantar todas as informações relevantes, verificando fatos e descartando boatos;
c) levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências;
d) avaliar a necessidade de suspender serviços e/ou sistemas informatizados;
e) centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;
f) realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas;
g) definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;
h) aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário do Estado do Ceará;
i) solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;
j) apoiar equipes de resposta e de recuperação com gerentes de crise experientes;
k) avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta;
l) orientar sobre as prioridades e estratégias da organização para recuperação rápida e eficaz;
m) definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e
n) elaborar plano de retorno à normalidade.

VII - todos os incidentes graves deverão ser comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça.

Art. 7º Melhoria contínua e lições aprendidas no pós-crise.

§ 1º Após o retorno das operações à normalidade, o CGSICC deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

§ 2º Para a identificação das lições aprendidas e a elaboração de relatório final, devem ser objeto de avaliação:

I - a identificação e análise da causa-raiz do incidente;
II - a linha do tempo das ações realizadas;
III - a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crises;
IV - os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;
V - o escalonamento da crise;
VI - a investigação e preservação de evidências;
VII - a efetividade das ações de contenção;
VIII - a coordenação da crise, liderança das equipes e gerenciamento de informações; e
IX - a tomada de decisão e as estratégias de recuperação.

§ 3º As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (*playbooks*) e para a melhoria do processo de preparação para crises cibernéticas.

§ 4º Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados. Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, e o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

ANEXO III DA PORTARIA Nº 2521/2022

PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO DO ESTADO DO CEARÁ (PIIC-PJCE)

Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário do Estado do Ceará (PIIC-PJCE)

Art. 1º O Protocolo de investigação para ilícitos cibernéticos estabelece os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

Art. 2º São definidos requisitos e procedimentos para coleta e preservação de evidências, bem como, deverá ser a comunicação do Incidente de Segurança Cibernética penalmente relevante.

Art. 3º Este protocolo complementa o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário do Estado do Ceará (PPINC-PJCE).

Art. 4º Fazem parte deste protocolo: requisitos para coleta e preservação de evidências, procedimento para coleta e preservação das evidências, comunicação do Incidente de segurança e o processo “Coletar e Preservar Evidências”.

Art. 5° Para coleta e preservação de evidências são necessários os seguintes requisitos:

I - adequação dos Ativos de Tecnologia da Informação:

a) horário dos ativos de tecnologia da informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON); e

b) os ativos de tecnologia da informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), tais como: autenticação, tanto as bem-sucedidas quanto as malsucedidas; acesso a recursos e dados privilegiados; e acesso e alteração nos registros de auditoria.

II - os registros dos eventos previstos no item “B” devem incluir as seguintes informações:

a) identificação inequívoca do usuário que acessou o recurso;

b) natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.;

c) data, hora e fuso horário, observando-se a HLB; e

d) endereço IP (Internet Protocol), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

III - os ativos de informação que não propiciem os registros dos eventos listados no item “C” devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

IV - os sistemas e as redes de comunicação de dados devem ser monitorados, registrando se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

a) utilização de usuários, perfis e grupos privilegiados;

b) inicialização, suspensão e reinicialização de serviços;

c) acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;

d) modificações da lista de membros de grupos privilegiados;

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

f) acesso ou modificação de arquivos ou sistemas considerados críticos; e

g) eventos obtidos por meio de quaisquer mecanismos de segurança existentes.

VI - os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (logs) em formato que possibilite a completa identificação dos fluxos de dados;

VII - os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos; e

VIII - os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, mas também remotamente, por meio do uso de tecnologia aplicável.

Art. 6º Procedimento para Coleta e Preservação das Evidências:

I - a ETIR, sob a supervisão de seu responsável, ou o Coordenador do CGETIC durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:

a) as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;

b) os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e

c) todos os registros de eventos citados neste documento.

II - nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR, sob a supervisão do seu responsável, ou o Coordenador do CGETIC deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os “metadados” desses arquivos, como data, hora de criação e permissões;

III - o agente responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados;

IV - as ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências;

V - para a preservação dos arquivos coletados, deve-se:

a) gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados;

b) gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea a deste subitem; e

c) gerar resumo criptográfico do arquivo a que se refere a deste subitem.

VI - todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante;

VII - o material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.

Art. 7º Da Comunicação do Incidente de Segurança:

I - assim que tomar conhecimento de Incidente de Segurança Cibernética penalmente relevante, deverá o responsável pelo órgão do Poder Judiciário afetado comunicá-lo de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos e ao Ministério Público;

II - considerado o incidente Crise Cibernética, o Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC) deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas;

III - após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados.

IV - o Relatório de Comunicação de Incidente de Segurança Cibernética deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:

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

b) nome do agente responsável pela ETIR e informações de contato;

c) órgão comunicante com sua localização e informações de contato;

d) número de controle da ocorrência;

e) relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados;

f) 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;

g) resumo criptográfico dos arquivos coletados;

h) termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

i) número de lacre de material físico preservado, se houver; e

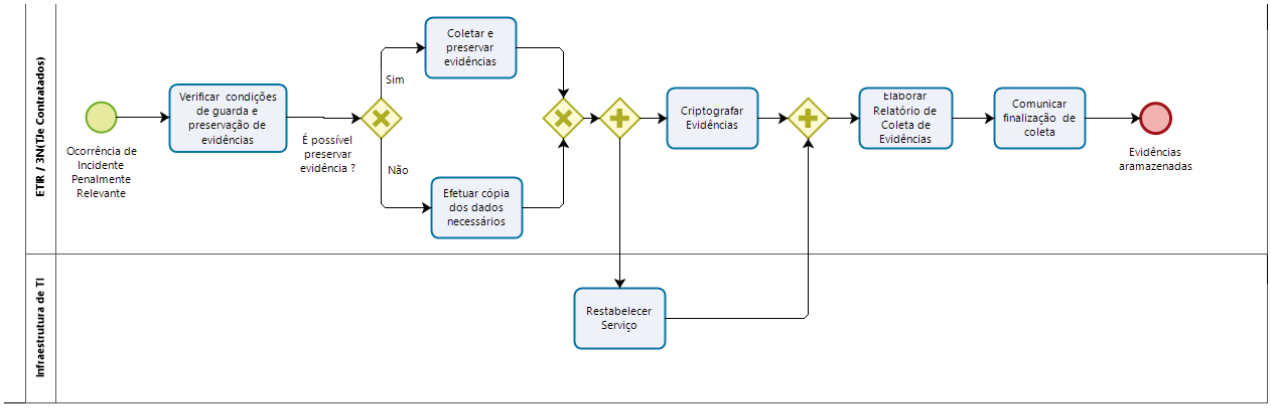
j) justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

V - o Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR, protocolado e encaminhado formalmente ao (à) Presidente do Poder Judiciário do Estado do Ceará;

VI - deverá constar no documento formal de encaminhamento a que se refere o item 4.5, apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos; e

VII - recebida a Comunicação de Incidente de Segurança em Redes Computacionais, o (à) Presidente do Poder Judiciário do Estado do Ceará deverá encaminhá-la formalmente 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. 8º Processo Coletar e Preservar Evidências:



PORTARIA Nº 2522/2022

Dispõe sobre atuação do Núcleo de Produtividade Remota.

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

RESOLVE:

Art. 1º Designar os(as) magistrados(magistradas) abaixo relacionados(as) para, no âmbito do Núcleo de Produtividade Remota, auxiliarem as varas infra relacionadas, no período de 19 de dezembro de 2022 a 31 janeiro de 2023:

Magistrado	Unidade Judiciária
Ana Claudia Gomes de Melo	Comarca Agregada de Jucás Comarca Agregada de Saboeiro
Daniel de Menezes Figueiredo Couto Bem	Comarca Agregada de Hidrolândia Vara Única da Comarca de Jijoca de Jericoacoara 3ª Vara Cível da Comarca de Juazeiro do Norte
Francisco Marcello Alves Nobre	Comarca Agregada de Morrinhos Comarca Agregada de Marco Vara Única da Comarca de Ipaumirim