18/12/2025

Número: **0600727-80.2025.6.16.0000**

Classe: **PROCESSO ADMINISTRATIVO**
Órgão julgador colegiado: **Colegiado do Tribunal Regional Eleitoral**
Órgão julgador: **Relatoria Presidência**
Última distribuição : **01/12/2025**
Valor da causa: **R$ 0,00**
Assuntos: **Proposta de Nova Resolução**
Objeto do processo: **Processo Administrativo nº 0600727-80.2025.6.16.0000 - Cuida-se de proposta de edição de portaria para instituir o Comitê de Crises Cibernéticas e os Protocolos de Prevenção a Incidentes Cibernéticos, de Gerenciamento de Crises Cibernéticas e de Investigação para Ilícitos Cibernéticos. SEI 0005836-83.2025.6.16.8000.**
Segredo de Justiça? **NÃO**
Justiça gratuita? **NÃO**
Pedido de liminar ou antecipação de tutela? **NÃO**

Partes	Advogados
TRIBUNAL REGIONAL ELEITORAL DO PARANA (INTERESSADO)	

Outros participantes	
Procurador Regional Eleitoral (FISCAL DA LEI)	

Documentos			
Id.	**Data da Assinatura**	**Documento**	**Tipo**
44809996	17/12/2025 19:10	Acórdão	Acórdão

TRIBUNAL REGIONAL ELEITORAL DO PARANÁ

ACÓRDÃO Nº 68.834

PROCESSO ADMINISTRATIVO 0600727-80.2025.6.16.0000 – Curitiba – PARANÁ
Relator: DES. SIGURD ROBERTO BENGTSSON
INTERESSADO: TRIBUNAL REGIONAL ELEITORAL DO PARANA
FISCAL DA LEI: Procurador Regional Eleitoral

RESOLUÇÃO Nº 962, DE 9 DE DEZEMBRO DE 2025.

Institui o Comitê de Crises Cibernéticas e os Protocolos de Prevenção de Incidentes Cibernéticos, de Gerenciamento de Crises Cibernéticas e de Investigação para Ilícitos Cibernéticos, no âmbito da Justiça Eleitoral do Paraná.

DECISÃO

À unanimidade de votos, a Corte aprovou a resolução, nos termos do voto do Relator.

Curitiba, 09/12/2025

RELATOR(A) DES. SIGURD ROBERTO BENGTSSON

O **TRIBUNAL REGIONAL ELEITORAL DO PARANÁ**, no uso das atribuições que lhe são conferidas pelo artigo 22, inciso VII, do seu Regimento Interno,

CONSIDERANDO o art. 50, § 2º, I, a, da Lei nº 13.709, de 14 de agosto de 2018 (LGPD);

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

CONSIDERANDO a Portaria CNJ nº 162, de 10 de junho de 2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021 e os termos do Anexo II, referente ao Protocolo Gerenciamento de Crises Cibernéticas do Poder Judiciário;

CONSIDERANDO a importância de prevenir e de minimizar os impactos negativos decorrentes de crises institucionais;

CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores;

CONSIDERANDO a necessidade de atuação com agilidade e segurança em caso de crise na instituição, para a manutenção ou retorno da regularidade dos serviços prestados à sociedade, sem descuidar da credibilidade do órgão;

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação para garantir a disponibilidade e integridade dos serviços e ativos tecnológicos do Tribunal Regional Eleitoral do Paraná;

CONSIDERANDO que a segurança da informação, a proteção e a privacidade de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Paraná;

CONSIDERANDO o contido no processo SEI nº 0005836-83.2025.6.16.8000,

RESOLVE

Art. 1º Instituir o Comitê de Crises Cibernéticas, o qual será composto por representantes das seguintes estruturas de governança e unidades do Tribunal Regional Eleitoral do Paraná, designados por meio de Portaria específica:

I - Presidência;

II - Diretoria-Geral;

III - Secretaria da Corregedoria Regional Eleitoral;

IV - Secretaria Judiciária;

V - Secretaria de Comunicação e Multimídia;

VI - Secretaria de Tecnologia da Informação;

VII - Secretaria de Administração;

VIII - Secretaria de Gestão de Pessoas;

IX - Secretaria de Orçamento, Finanças e Contabilidade;

X - Secretaria de Auditoria Interna;

XI - Secretaria de Planejamento e Logística de Eleições;

XII - Coordenadoria de Segurança, Inteligência Artificial e Governança de TI;

XIII - Assessoria de Segurança Cibernética;

XIV - Assistência de LGPD e Processos Institucionais;

XV - Gestor(a) de Segurança da Informação;

XVI - Agente responsável pela ETIR;

XVII - Encarregado(a) de Dados;

XVIII - Gabinete das Ouvidorias.

Art. 2.º O Comitê de Crises Cibernéticas atuará nos casos previstos no ANEXO II desta Portaria, observando as atribuições nele estabelecidas, e será presidido pelo(a) titular da Secretaria de Tecnologia da Informação.

§ 1.º Fica definida a Sala de Reuniões da Secretaria de Tecnologia da Informação como sala de situação, local a partir do qual serão geridas as crises cibernéticas.

§ 2.º Na impossibilidade de utilização da Sala de Reuniões da Secretaria de Tecnologia da Informação, as deliberações sobre o incidente que constitui a crise cibernética serão tomadas, preferencialmente, mediante reunião virtual por meio de solução oficial de videoconferência adotada pelo Tribunal.

§ 3.º A sala de situação deve dispor dos meios necessários, inclusive de sistemas de áudio, vídeo e chamadas telefônicas, e estar próxima a um local onde se possa fazer declarações públicas à imprensa.

Art. 3.º O Comitê de Crises Cibernéticas poderá solicitar o suporte da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e de Segurança Cibernética (ETIR) e de especialistas das áreas Jurídica, Comunicação Institucional, Tecnologia da Informação e Comunicação, Privacidade de Dados Pessoais, Segurança da Informação, Administrativas de Apoio à Contratação e Segurança Institucional.

Art. 4.º O Comitê de Crises Cibernéticas deverá ser acionado sempre que for identificada uma crise cibernética.

§ 1.º O acionamento do Comitê poderá se dar pelo(a) Presidente do Tribunal, por seu(sua) Vice-Presidente e Corregedor(a), pelo(a) Diretor(a)-Geral e pelos integrantes do Comitê, caso constatem indícios de concretização ou de iminência de concretização de riscos que possam impactar o Tribunal como um todo.

§ 2.º O Comitê de Crises Cibernéticas, quando acionado, será coordenado pelo(a) titular da Coordenadoria de Segurança, Inteligência Artificial e Governança de TI.

§ 3.º No desempenho de suas atribuições institucionais, o Comitê de Crise Cibernética deverá observar as diretrizes da Política de Segurança da Informação (PSI) da Justiça Eleitoral, e atuar de forma coordenada com o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais (CGSIPDP).

§ 4.º As deliberações e propostas do Comitê de Crise Cibernética deverão estar em consonância com os normativos e recomendações do Conselho Nacional de Justiça (CNJ), do Tribunal Superior Eleitoral (TSE) e do Tribunal Regional Eleitoral do Paraná (TRE-PR) e as deliberações serão motivadas e aprovadas, com registro em Ata em processo no SEI.

Art. 5.º O Comitê de Crises Cibernéticas terá as seguintes atribuições:

I - adotar medidas de contingência para a continuidade dos serviços prestados, sempre que acionado pela ETIR, em caso de crise cibernética;

II - analisar as informações referentes ao incidente prestadas pela ETIR e pela(s) área(s) técnica(s) envolvida(s) da Secretaria de Tecnologia da Informação (SECTI);

III - decidir sobre a suspensão de serviços ou sistemas;

IV - aplicar o Protocolo de Investigação para Ilícitos Cibernéticos;

V - gerenciar a comunicação;

VI - deliberar sobre o plano de restabelecimento dos serviços afetados, elaborado pela ETIR;

VII - realizar análise criteriosa das ações adotadas durante a crise cibernética, após o restabelecimento dos serviços, considerando aspectos como: causa raiz do incidente, impacto nos dados, sistemas e operações, processos de detecção, proteção e estratégias de recuperação;

VIII - deliberar sobre o relatório elaborado pela ETIR, que conterá a descrição e o detalhamento do incidente, bem como as ações adotadas ao final de cada incidente de crise cibernética, tendo por objetivo documentar as práticas adotadas para servir de referência na resolução de possíveis novos incidentes.

Art. 6.º Ficam instituídos os protocolos de segurança cibernética, definidos na Resolução CNJ nº 396/2021 e detalhados na Portaria CNJ nº 162/2021, constantes dos seguintes anexos:

I - ANEXO I - Protocolo de Prevenção de Incidentes Cibernéticos (PPINC);

II - ANEXO II - Protocolo de Gerenciamento de Crises Cibernéticas (PGCC);

III - ANEXO III - Protocolo de Investigação para Ilícitos Cibernéticos (PIILC).

Art. 7.º Para os efeitos desta Resolução e de seus anexos, aplicar-se-á, como referência, o glossário de termos e definições estabelecido no Anexo VIII, da Portaria CNJ nº 162/2021 (página 100 à 107).

Art. 8.º Os protocolos deverão ser disponibilizados no site do Tribunal.

Art. 9.º Os protocolos estabelecidos serão revistos no segundo semestre de anos ímpares, ou quando necessário, mediante sugestão do(a) Presidente do Comitê de Crises Cibernéticas.

Art. 10. Esta Resolução entra em vigor na data de sua publicação.

SESSÃO DE JULGAMENTO DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, em 9 de

DEZEMBRO de 2025.

Des. SIGURD ROBERTO BENGTSSON

Presidente

Des. LUIZ OSÓRIO MORAES PANZA

Vice-Presidente e Corregedor Regional Eleitoral

Desª. Federal CLAUDIA CRISTINA CRISTOFANI

Des. Eleitoral JOSÉ RODRIGO SADE

Des. Eleitoral OSVALDO CANELA JÚNIOR

Desª. Eleitoral VANESSA JAMUS MARCHI

Desª. Eleitoral Substituta TATIANE DE CÁSSIA VIESE

Dr. MARCELO GODOY

Procurador Regional Eleitoral

ANEXO I

PROTOCOLO DE PREVENÇÃO DE INCIDENTES CIBERNÉTICOS

1. Disposições Preliminares.

1.1 O Protocolo de Prevenção de Incidentes Cibernéticos (PPINC) tem por objetivo:

I - prevenir incidentes cibernéticos por meio das funções: identificar, proteger, detectar, responder e recuperar;

II - promover alinhamento às normas, regulamentações e às melhores práticas, relacionadas à gestão de incidentes de segurança da informação;

III - promover ações que contribuam para a resiliência dos serviços de tecnologia da informação a ataques cibernéticos.

1.2 O Protocolo de Investigação para Ilícitos Cibernéticos (PIILC) e o Protocolo de Gerenciamento de Crises Cibernéticas (PGCC) são complementares e harmonizam-se com este Protocolo de Prevenção de Incidentes Cibernéticos.

1.3 Para implementação desta norma, as áreas envolvidas deverão observar os princípios críticos definidos no Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário - PPINC-PJ, que são:

I - uso da base de conhecimento de defesa;

II - priorização da segurança cibernética;

III - instrumentos de medição e métricas;

IV - diagnóstico contínuo;

V - formação, capacitação e conscientização;

VI - busca de soluções automatizadas de segurança cibernética;

VII - resiliência.

1.4 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e de Segurança Cibernética (ETIR) é instituída por Portaria da Diretoria-Geral.

2. Competência de atuação.

2.1 Cabe à Diretoria-Geral:

I - analisar as deliberações do Comitê Gestor de Segurança da Informação e de Proteção de Dados Pessoais sobre gestão de incidentes de segurança da informação e decidir sobre possíveis providências;

II - formalizar a aceitação da execução das ações propostas para conter ou prevenir incidentes de segurança da informação;

III - comunicar fatos potencialmente relevantes ao(à) Presidente do Tribunal, para eventual encaminhamento aos órgãos de investigação com atribuição para o início da persecução penal;

IV - acionar o Comitê de Crises Cibernéticas, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, quando necessário.

2.2 Cabe ao Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais, sem prejuízo de

outras atribuições estabelecidas em regulamentação específica:

I - deliberar sobre as principais diretrizes e temas relacionados à Gestão de Incidentes de Segurança da Informação;

II - avaliar periodicamente a estrutura de Gestão de Incidentes de Segurança da Informação e os respectivos controles internos, assim como propor melhorias consideradas necessárias;

III - propor o Processo de Gestão de Incidentes de Segurança da Informação e suas futuras revisões.

2.3 Cabe às unidades vinculadas à Secretaria de Tecnologia da Informação:

I - monitorar e comunicar à ETIR os incidentes de segurança da informação dos ativos sob sua responsabilidade;

II - assegurar a implementação das ações e dos controles definidos para prevenção e contenção de incidentes de segurança da informação dos ativos sob sua responsabilidade.

2.4 Cabe à unidade de Segurança Cibernética da Secretaria de Tecnologia da Informação (SECTI):

I - testar e implementar o Processo de Gestão de Incidentes de Segurança da Informação no escopo da segurança cibernética, visando assegurar a sua efetividade;

II - disseminar a cultura voltada para comunicação de incidentes de segurança cibernética;

III - subsidiar o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais, com informações pertinentes à estrutura e gestão de incidentes de segurança cibernética.

3. Funções do Protocolo de Prevenção de Incidentes Cibernéticos.

3.1 São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos, conforme definição do PPINC-PJ: identificar, detectar, responder o incidente, proteger e recuperar a informação.

3.2 Função Identificar.

3.2.1 A função "Identificar" consiste na análise dos riscos de ataques cibernéticos a que sistemas, pessoas, dados, recursos e ativos de TIC (Tecnologia da Informação e Comunicação) em geral estão expostos, incluindo a elaboração e a execução de um plano de tratamento dos riscos.

3.2.2 A função "Identificar" é executada dentro do escopo do Processo de Gestão de Riscos de Segurança da Informação do Tribunal.

3.3 Função Proteger.

3.3.1 A função "Proteger" consiste no desenvolvimento e na implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, de ativos de informação, bem como a prestação de serviços críticos.

3.3.2 A função "Proteger" deve ser implementada pelo conjunto mínimo de ações elencadas a seguir:

I - implantação e aprimoramento contínuo de um sistema de gestão de segurança da informação;

II - controle de acesso e de utilização de recursos de TIC;

III - cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos;

IV - plano de continuidade dos serviços essenciais de TIC;

V - gestão de capacidade e disponibilidade dos serviços essenciais de TIC;

VI - processo de gerenciamento de mudança para todos os ativos de TIC;

VII - gestão de vulnerabilidade dos serviços essenciais de TIC;

VIII - utilização de ferramenta de segurança para estações de trabalho, contendo, no mínimo, as funções de antivírus, automação de políticas de segurança de endpoint, proteção contra criptografia de arquivos (ransomware), controle de aplicativos e de dispositivos removíveis;

IX - controle de acesso a conteúdo na internet (filtragem web);

X - utilização de ferramenta de segurança de rede (next generation firewall), para filtragem e bloqueio de tráfego de rede, prevenção de ameaças e implementação de redes privadas virtuais (VPN);

XI - uso de antivírus de rede, sistema de detecção e prevenção de ameaças e implementação de redes privadas virtuais (VPN);

XII - integridade da rede protegida por meio da segmentação e segregação de ambientes, de maneira a estabelecer barreiras de contenção de danos em caso de comprometimento (sub-redes distintas por serviços) e para garantia de recursos para serviços prioritários (serviços essenciais, em detrimento de ambientes de laboratório/desenvolvimento/homologação);

XIII - promover campanha e/ou treinamento sobre segurança da informação para magistrados e servidores;

XIV - atualização tecnológica constante;

XV - implementação gradual das melhores práticas de controle de segurança da informação, a exemplo das presentes na Norma NBR 27002;

XVI - implementação gradual dos controles mínimos recomendados no Manual de Referência - Proteção de Infraestruturas Críticas de TIC, editado pelo Conselho Nacional de Justiça, considerando a escala de aplicabilidade de cada controle em relação ao porte e maturidade do TRE-PR em segurança cibernética;

XVII - implementação gradual dos requisitos de resiliência cibernética, recomendados no Manual de Referência - Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TRE-PR em segurança cibernética;

XVIII - implementação gradual dos requisitos de resiliência cibernética recomendados no Manual de Referência - Gestão de Identidade e de Controle de Acessos, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TRE-PR em segurança cibernética;

XIX - implantação gradual de uma política de educação e cultura em segurança cibernética, conforme o Anexo VII da Portaria CNJ nº 162/2021.

3.3.3 As salvaguardas elencadas no item 3.3.2 devem ser implementadas para todos os ativos de TIC, no que couber, considerados essenciais ou não ao negócio, permitindo variar quanto ao nível de implementação, de acordo com a natureza e criticidade do ativo.

3.3.4 As atualizações dos ativos de TIC (pacotes de segurança, firmware, entre outros) devem ser aplicadas, sempre que possível, tão logo liberadas, mas considerando:

I - os riscos decorrentes da atualização;

II - os riscos decorrentes da não aplicação (ou postergação);

III - a criticidade do ativo;

IV - a estabilidade dos serviços.

3.4 Funções Detectar, Responder e Recuperar.

3.4.1 As atividades decorrentes das funções "Detectar", "Responder" e "Recuperar" do Protocolo de Prevenção de Incidentes Cibernéticos devem estar cobertas pelo Processo de Gestão de Incidentes de Segurança da Informação.

3.4.2 Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, deverá, ainda, ser seguido o Protocolo de Investigação para Ilícitos Cibernéticos.

3.4.2.1 Na ocorrência da hipótese prevista, o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais e a Presidência deverão ser comunicados pela ETIR.

3.4.3 Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

3.4.4 A gestão de incidentes de segurança cibernética deve ser realizada por meio do Processo de Gestão de Incidentes de Segurança da Informação, contendo as fases de detecção, triagem, análise e respostas aos incidentes de segurança.

3.4.5 As ações relacionadas à prevenção de incidentes devem observar, ainda, o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), constante do Anexo I da Portaria CNJ nº 162/2021.

ANEXO II

PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS

1. Disposições Preliminares.

1.1 O Protocolo de Gerenciamento de Crises Cibernéticas é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos e define 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.

1.2 O gerenciamento de incidentes refere-se às atividades que devem ser executadas em face da ocorrência de evento adverso de segurança da informação, para avaliar o problema e determinar a resposta inicial.

1.3 O Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC) definirá a lista de

serviços essenciais que serão considerados críticos ao funcionamento do Tribunal, para efeito deste protocolo.

2. Fase de Planejamento (pré-crise).

2.1 Para melhor lidar com uma crise cibernética, é necessária prévia e adequada preparação, sendo fundamental manter um Programa de Gestão de Continuidade de Serviços de TIC.

2.2 O gerenciamento de crise se inicia quando:

I - restar caracterizado grave dano material ou à imagem institucional;

II - for evidenciada a possibilidade de que as ações de resposta ao incidente cibernético irão persistir por longo período;

III - o incidente impactar gravemente os serviços de TIC essenciais ao funcionamento do Tribunal, extrapolando os limites determinados nas diretrizes do plano de continuidade de serviços de TIC do TRE-PR;

IV - o incidente atrair grande atenção da mídia e da população em geral;

V - ocorrer vazamento de quantidade significativa de dados pessoais.

3. Fase de Execução (durante a crise).

3.1 Caso o incidente de segurança constitua uma crise cibernética, caberá à ETIR comunicar o fato ao Comitê de Crises Cibernéticas, que deverá se reunir imediatamente para tomada de decisões acerca do incidente.

3.2 Caso seja confirmada a crise cibernética, o Comitê de Crises Cibernéticas entrará em estado de convocação permanente, podendo se reunir a qualquer horário para discutir, deliberar e agir no tratamento da crise em curso.

3.3 O acesso às reuniões do Comitê de Crises Cibernéticas deve ser restrito aos membros do Comitê e aos atores eventualmente convidados a participar das reuniões.

3.4 O Comitê de Crises Cibernéticas deve ter acesso ágil a meios que o permita fazer declarações públicas à imprensa.

3.5 O Comitê de Crises Cibernéticas deve alocar uma equipe dedicada à execução de atividades administrativas e técnicas necessárias durante o período de crise.

3.6 Os planos de contingências existentes, caso aplicáveis, devem ser efetivados imediatamente após a declaração da crise cibernética, visando à continuidade dos serviços prestados pelo TRE-PR.

3.7 Para eficácia do trabalho do Comitê de Crises Cibernéticas, é necessário que os esforços visem:

I - entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;

II - levantar todas as informações relevantes, verificando fatos, descartando e mitigando boatos;

III - levantar soluções para a crise e deliberar sobre a viabilidade e consequências das alternativas identificadas;

IV - avaliar a necessidade de suspender serviços e/ou sistemas informatizados afetados;

V - estabelecer um interlocutor a fim de centralizar a comunicação para evitar informações equivocadas ou imprecisas;

VI - realizar uma comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e evitar boatos ou investigações paralelas que alimentem notícias falsas;

VII - definir estratégias de comunicação com a Secretaria de Comunicação e Multimídia, sendo esta unidade a única fonte autorizada a estabelecer a estratégia de comunicação mais adequada;

VIII - aplicar o Protocolo de Investigação para Ilícitos Cibernéticos;

IX - solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;

X - apoiar as equipes de resposta e de recuperação com gerentes de crise experientes;

XI - realizar comunicação direta e imediata à Secretaria de Tecnologia da Informação do Tribunal Superior Eleitoral ou ao representante do Comitê de Crises Cibernéticas daquele Tribunal Superior Eleitoral, visando a mitigação dos riscos de propagação do incidente para outros órgãos da Justiça Eleitoral;

XII - avaliar a necessidade de recursos adicionais extraordinários para apoiar as equipes de resposta;

XIII - fornecer aconselhamento sobre as prioridades e estratégias da organização para uma recuperação rápida e eficaz;

XIV - definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações, com base nos dados obtidos sobre o incidente;

XV - elaborar plano de restabelecimento dos serviços impactados.

3.8 As etapas e procedimentos de resposta são diferentes, a depender do tipo de crise, e são necessárias reuniões regulares, para avaliar o progresso, até que seja possível restabelecer os serviços impactados.

3.9 A Presidência do TRE-PR encaminhará as comunicações oficiais da ocorrência do incidente grave quando constatada uma crise cibernética:

I - ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça;

II - ao Ministério Público Federal (MPF) e à Ordem dos Advogados do Brasil, Seção Paraná (OAB/PR), quando o incidente envolver a prestação jurisdicional.

3.10 Cabe ao(à) encarregado(a) de tratamento de dados pessoais comunicar aos titulares de dados pessoais, a ocorrência de incidente grave, envolvendo dados pessoais, que possa acarretar risco ou dano relevante aos titulares.

3.11 Cabe à Secretaria de Tecnologia da Informação:

I - identificar e manter documentação técnica atualizada dos ativos de informação que suportam os serviços essenciais;

II - avaliar e tratar os riscos de TIC aos quais as atividades estratégicas estão expostas e que possam impactar diretamente na continuidade do negócio, de acordo com o Processo de Gestão de Riscos de Segurança da Informação;

III - acompanhar a execução do plano de gestão de incidentes cibernéticos dos ativos críticos, o qual deve possuir, no mínimo, as categorias de incidentes a que os ativos críticos estão sujeitos; a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência de incidente; e a severidade do incidente;

IV - supervisionar a elaboração e os testes dos planos de contingência de TIC para os serviços essenciais, sem prejuízo das ações decorrentes da norma complementar que estabelece as diretrizes para a gestão da continuidade de serviços de TIC do TRE-PR.

4. Fase de Aprendizado e Revisão (Pós-Crise)

4.1 Quando os serviços afetados forem restabelecidos, o Comitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

4.2 Deve ser objeto de avaliação para a identificação das lições aprendidas:

I - a identificação e análise da causa do incidente cibernético;

II - a linha do tempo das ações realizadas;

III - a escala do impacto nos dados, sistemas e operações de serviços críticos durante a crise;

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;

IX - a tomada de decisão e as estratégias de recuperação.

4.3 As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (playbook) e para a melhoria do processo de preparação para crises cibernéticas.

4.4 Deve ser elaborado relatório final pelo Comitê de Crises Cibernéticas, contendo a descrição e detalhamento da crise, bem como o plano de ação adotado, para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

4.5 As ações de resposta e recuperação da crise cibernética devem observar, ainda, o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ), constante do Anexo II da Portaria CNJ nº 162/2021.

ANEXO III

PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS

1. O Protocolo de Investigação para Ilícitos Cibernéticos tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências, bem como para comunicar fatos potencialmente relevantes aos órgãos de investigação e com atribuição para o início da persecução penal.

2. Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e de Segurança Cibernética (ETIR), durante o processo de tratamento de incidente penalmente relevante, sem prejuízo de outras ações estabelecidas no normativo que a institui:

I - conduzir o tratamento do incidente, observando os procedimentos para coleta e preservação das evidências, definidos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário, quando o incidente for penalmente relevante;

II - comunicar o fato ao Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais;

III - comunicar ao(à) encarregado(a) pelo tratamento de dados pessoais do TRE-PR, quando o incidente envolver dados pessoais.

2.1 O Comitê Gestor de Segurança da Informação e de Proteção de Dados Pessoais deverá comunicar o fato à Presidência.

2.2 O(a) encarregado(a) pelo tratamento de dados pessoais do TRE-PR, deverá comunicar o incidente aos titulares de dados pessoais que tiverem seus dados vazados e, se entender necessário, à Agência Nacional de Proteção de Dados Pessoais (ANPD).

2.3 O Comitê de Crises Cibernéticas deverá ser acionado sempre que o incidente for considerado como crise cibernética.

3. As ações de coleta e preservação de evidências devem observar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ), constante do Anexo III da Portaria CNJ nº 162/2021.

EXTRATO DA ATA

PROCESSO ADMINISTRATIVO(1298) Nº 0600727-80.2025.6.16.0000 - Curitiba - PARANÁ - RELATOR: DES. SIGURD ROBERTO BENGTSSON - INTERESSADO: TRIBUNAL REGIONAL ELEITORAL DO PARANA

DECISÃO

À unanimidade de votos, a Corte aprovou a resolução, nos termos do voto do relator.

Presidência do excelentíssimo senhor desembargador Sigurd Roberto Bengtsson. Participaram do julgamento os eminentes julgadores: desembargadora federal Claudia Cristina Cristofani, desembargador Luiz Osório Moraes Panza, e os desembargadores eleitorais, José Rodrigo Sade, Osvaldo Canela Junior,

Vanessa Jamus Marchi e Tatiane de Cassia Viese. Presente o procurador regional eleitoral, Marcelo Godoy.

SESSÃO DE 09.12.2025.