INTRUÇÃO NORMATIVA N° 206/2026

SUMÁRIO

INSTRUÇÃO NORMATIVA N° 206/2026

Dispõe sobre o Plano de Gestão e Resposta de Incidentes de Segurança da Informação no Tribunal de Contas do Estado do Paraná, em conformidade com a Política de Segurança da Informação e Comunicações, e dá outras providências.

O **TRIBUNAL DE CONTAS DO ESTADO DO PARANÁ,** no uso das atribuições institucionais estabelecidas na Constituição Estadual e com base no art. 2º, I, da Lei Complementar Estadual nº 113, de 15 de dezembro de 2005, e nos arts. 5º, XIII, 187, II, 193, parágrafo único, 194, 196 do Regimento Interno, bem como no art. 31 da Resolução nº 120, de 16 de setembro de 2024, e considerando o Acórdão nº 657/26-Tribunal Pleno, Processo nº 710938/25,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º Esta Instrução Normativa dispõe sobre o Plano de Gestão e Resposta de Incidentes de Segurança da Informação (ISI) no Tribunal de Contas do Estado do Paraná (TCE-PR), em conformidade com a Política de Segurança da Informação e Comunicações.

Parágrafo único. O objetivo do Plano de Gestão e Resposta de Incidentes de Segurança da Informação é fornecer uma estrutura clara e abrangente para prevenir, detectar, avaliar, responder e recuperar de forma eficaz e eficiente os incidentes de cibersegurança, minimizando danos e interrupções aos sistemas, dados e operações do tribunal, assim como estabelecer a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos no Tribunal de Contas do Paraná.

CAPÍTULO II
DOS TERMOS E DEFINIÇÕES

Art. 2º Para os fins desta Instrução Normativa, considera-se:

I - Evento de Incidente de Segurança da Informação (ISI): quaisquer eventos que representem uma ameaça à confidencialidade, integridade ou disponibilidade de informações ou sistemas da organização, indicando uma violação da política de segurança da informação ou falha de seus controles, ou uma situação previamente desconhecida que possa ser relevante e que têm uma probabilidade significativa de comprometer as operações do negócio e de ameaçar a segurança da informação;

II - Classificação de Incidentes: atribuição de níveis de gravidade aos incidentes, geralmente divididos em categorias, como baixa, média, alta e crítica;

III - Etapas de Resposta a Incidentes: atividades sequenciais para identificar, conter, erradicar, recuperar e documentar um incidente.

CAPÍTULO III
DOS PAPEIS E RESPONSABILIDADES

Art. 3º A equipe de resposta a incidentes de segurança da informação deve incluir membros com habilidades técnicas e conhecimentos específicos em cibersegurança. As principais funções e responsabilidades são:

I - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR): grupo de profissionais designados pela DTI para planejar, coordenar, mitigar e executar a resposta a incidentes cibernéticos;

II - Coordenador de Incidentes: responsável por liderar a ETIR e coordenar a resposta a incidentes de segurança da informação, a cargo do gerente de cibersegurança;

III - Analista de Segurança: encarregado de analisar os incidentes, identificar a origem, identificar a abrangência do incidente, determinar e executar ações corretivas iniciais. Este analista pode ser integrante de equipes terceirizada *do Security Operations Center* – SOC do TCE-PR;

IV - Analista de Suporte: responsável por isolar sistemas comprometidos, mitigar vulnerabilidades e restaurar a funcionalidade. Pode ser integrante de equipe terceirizada de Suporte Especializado;

V - Jurídico/*Compliance*: avalia implicações legais e regulatórias e ajuda na notificação de incidentes, quando necessário, com o apoio da Diretoria Jurídica;

VI - Comunicação: Gerencia a comunicação interna e externa, incluindo a mídia e partes interessadas, com o apoio da Diretoria de Comunicação Social.

Art. 4º Os tipos de incidentes cibernéticos a serem notificados podem ser, mas não se limitam a:

I - abuso de sítios (desfiguração/*defacement*, injeção de *links*/código - *spamdexing*, erros de código, *cross-site scripting*, abuso de fórum ou livros de visita, etc.);

II - inclusão remota de arquivos (*remote file inclusion* - RFI) em servidores *web*;

III - uso abusivo de servidores de *e-mail*;

IV - hospedagem ou redirecionamento de artefatos ou código malicioso;

V - ataques de negação de serviço (DoS, DDoS, DRDoS);

VI - uso ou acesso não autorizado a sistemas ou dados;

VII - varredura de portas (*Port Scan*);

VIII - comprometimento de computadores ou redes;

IX - desrespeito à Política de Segurança da Informação/Cibernética ou uso inadequado dos recursos de Tecnologia da Informação (TI);

X - ataques de engenharia social (*Phishing*);

XI - cópia e distribuição não autorizadas de material protegido por direitos autorais;

XII - uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes;

XIII - ataques contra sistemas de autenticação (*Brute Force Attack*);

XIV - indisponibilidade de ativos por criptografia (*Ransomware Attack*);

XV - exploração de vulnerabilidades;

XVI - vazamentos de dados (*Data Leak*); e

XVII - outros incidentes cibernéticos.

CAPÍTULO IV
DO PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 5º O processo de Resposta a Incidentes de Segurança da Informação será baseado nas diretrizes e melhores práticas para gerenciamento de incidentes cibernéticos e será composto pelas seguintes etapas:

I - Preparação;

II - Detecção e Análise de Incidentes;

III - Contenção, Erradicação e Recuperação;

IV - Atividades Pós-Eventos de Incidentes; e

V – Revisão da Resposta

Seção I
Da Preparação

Art. 6º A etapa de preparação engloba as tarefas voltadas para mitigar e se antecipar à resposta a incidentes cibernéticos, envolvendo o estabelecimento adequado de ferramentas, alocação de recursos apropriados e proporcionando treinamento à equipe.

Parágrafo único. Dentro desse contexto, essa fase também compreende esforços para prevenir a ocorrência dos seguintes incidentes:

I - identificar ativos críticos: a identificação de ativos críticos envolve realizar o inventário abrangente de todos os ativos de TI do TCE-PR, incluindo *hardware*, *software*, dados, redes, sistemas, e qualquer outro componente relevante;

II - categorizar ativos críticos com base em sua importância operacional e estratégica para o funcionamento e continuidade das operações do TCE-PR;

III - definir políticas e procedimentos: a ETIR deverá elaborar documentação detalhada para atuação em cada tipo de ataque cibernético e, por medida de segurança, a documentação detalhada referente ao tratamento dos diferentes tipos de ataques e incidentes cibernéticos, estará disponível e de fácil acesso a todos integrantes da ETIR apenas.

Seção II
Da Detecção e Análise de Incidentes

Art. 7º Esta etapa consiste em identificar e confirmar a ocorrência do incidente de cibersegurança, incluindo a análise nos sistemas de detecção e monitoramento, assim como a definição da extensão dos incidentes no ambiente computacional, que são:

I - Detectar: devem ser utilizados sistemas de detecção de intrusões, monitoramento de *logs* e outras ferramentas para identificar incidentes que tenham a capacidade de monitorar e rastrear problemas recorrentes e novos, com repositório de informações referentes a incidentes tratados anteriormente e suas respectivas evidências de tratamento;

II - Realizar Avaliação Preliminar: através das ferramentas acima, determine em conjunto com demais integrantes da ETIR, a gravidade e o escopo do incidente, podendo se utilizar uma equipe com um canal específico no *MS-Teams* para as comunicações entre as diversas equipes envolvidas.

Seção III
Da Contenção, Erradicação e Recuperação

Art. 8º Esta etapa consiste em limitar o impacto do incidente, eliminando a ameaça, restaurar sistemas e serviços afetados, bem como verificar a eficácia das ações tomadas:

I - Isolar: verificar a necessidade de isolar sistemas e contas de usuário afetados para evitar a propagação do incidente, principalmente para os incidentes de gravidade alta e crítica;

II - Identificar Causa-Raiz: identificar como o incidente ocorreu e como a ameaça foi explorada, verificando os *logs* e a cadeia de ataque;

III - Erradicar: remover completamente a ameaça e as vulnerabilidades associadas e, em caso de impossibilidade de remoção completa da ameaça, deve ser feito o isolamento do ativo e, se necessário, da conta de usuário específica da qual se originou o ataque;

IV - Acionar Suporte Especializado: em caso de necessidade de atuação do suporte especializado nível 3, além do contato em canal específico no *MS-Teams,* deverá ser feita a abertura de chamado no ITSM (GLPI) específico referente a “incidente de segurança da informação” para que a equipe técnica especializada possa atuar;

V - Recuperação, abrangendo:

a) Restauração de Sistemas: restaurar sistemas afetados a um estado operacional seguro.

b) Verificação de Integridade: certificar-se de que os sistemas recuperados não foram ou estão comprometidos antes de liberação para o uso.

Seção IV
Das Atividades Pós-Eventos de Incidentes

Art. 9º Nesta etapa, devem ser realizadas ações voltadas para a aprendizagem e para garantir a melhoria contínua da capacidade de identificar, responder e se recuperar de incidentes de cibersegurança, contribuindo para uma postura geral mais robusta e assertiva contra ameaças, na forma seguinte:

I - Avaliação da Resposta ao Incidente: deve ser feita uma análise crítica de como a ETIR lidou com o incidente, avaliando-se a eficácia das ações tomadas durante as fases anteriores, identificando pontos fortes e áreas que podem ser aprimoradas;

II - Análise Pós-Incidente: realizar uma avaliação mais aprofundada das causas raízes do incidente, principalmente os de gravidade crítica e alta, buscando entender as origens e os métodos utilizados pelos invasores. Isso contribui para fortalecer as defesas e prevenir incidentes similares no futuro;

III - Documentação de Lições Aprendidas: Registrar o conhecimento adquirido durante e após o incidente, destacando o que funcionou bem e o que poderia ser melhorado. Essa documentação é valiosa para orientar futuras respostas a incidentes e treinamentos;

IV - Ajustes em Políticas e Procedimentos: Com base nas lições aprendidas, verificar a necessidade de atualizar a políticas, procedimentos e planos de resposta a incidentes, ajudando a manter a resiliência da segurança cibernética do tribunal diante de ameaças que estão em constante evolução;

V - Encerramento – Documentação Final: o registro final de todas as ações tomadas e os resultados são importantes insumos para o registro das lições aprendidas e disseminação do conhecimento de forma a mitigar eventos semelhantes que possam surgir.

Seção V
Da Revisão Da Resposta

Art. 10. A revisão pós-eventos de incidentes deve ser realizada para avaliar a eficácia da resposta.

§ 1º Este plano deve ser mantido atualizado e ser complementado por simulações e treinamentos regulares para garantir a preparação contínua da organização para incidentes de segurança da informação.

§ 2º Além disso, a equipe de resposta a incidentes deve estar ciente das leis e regulamentações externas e internas de privacidade de dados que podem exigir notificação às autoridades ou partes afetadas em caso de violação de dados.

CAPÍTULO V
DO PLANO DE COMUNICAÇÃO

Art. 11. Para o Plano de Comunicação, são necessárias as seguintes providências:

I - um plano de comunicação para incidentes de cibersegurança, principalmente para os incidentes de gravidade alta e crítica que possam afetar a missão institucional do Tribunal, pode ser necessário para lidar com a situação de forma eficaz, minimizando o impacto de ruído nas comunicações e restaurando a confiança das partes interessadas;

II - Notificação: conforme a gravidade do incidente, as partes interessadas internas e externas, devem ser informadas imediatamente;

III - vazamento de Dados Pessoais: em caso de incidentes de cibersegurança de gravidade alta ou crítica envolvendo dados pessoais, o DPO (Encarregado de Dados Pessoais do TCE-PR) deve ser informado imediatamente para que sejam tomadas as ações pertinentes junto aos órgãos competentes;

IV - Comunicação Externa: em casos de incidentes de segurança da informação considerados críticos, pode ser preparado uma estratégia de comunicação com a mídia e público externo, de forma a manter a sociedade ciente da continuidade das atividades do TCE-PR e o plano de recuperação a ser seguido.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 12. O não cumprimento desta Instrução Normativa pode resultar em procedimentos disciplinares aos responsáveis, conforme a legislação específica.

Parágrafo único. Além das medidas constantes do *caput*, o Tribunal pode tomar medidas legais em caso de violações graves de segurança de dados.

Art. 13. A revisão da presente Instrução Normativa ocorrerá sempre que se fizer necessária ou conveniente para o Tribunal, não excedendo o período máximo de três anos.

Parágrafo único. A não observação do prazo máximo para revisão pode resultar em procedimentos disciplinares cabíveis aos responsáveis pela área e pela unidade, conforme a legislação específica.

Art. 14. As necessárias inclusões, exclusões ou alterações referentes aos Anexos desta Instrução Normativa devem ser feitas mediante instauração de procedimento administrativo de projeto de instrução normativa, feito pela unidade técnica, acompanhado das motivações e conforme a padronização de atos normativos.

Art. 15. Esta Instrução Normativa entra em vigor na data da sua publicação.

Curitiba, 23 de abril de 2026.

- assinatura digital -

Conselheiro **IVAN LELIS BONILHA**

Vice-Presidente no exercício da Presidência