TRIBUNAL DE JUSTIÇA - ATOS DO PRESIDENTE

INSTRUÇÃO NORMATIVA 00002/2026 **Disponibilização: 29/09/2026 às 17h43m**

INSTRUÇÃO NORMATIVA Nº 2/2026-GABPRESI

Detalha os critérios de classificação de incidentes de segurança da informação e os procedimentos de escalonamento e comunicação correspondentes a cada nível de severidade, nos termos do § 3º do art. 9º da Portaria nº 2303/2026.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ (TJCE), no uso de suas atribuições legais e regimentais,

RESOLVE:

CAPÍTULO I

DOS CRITÉRIOS DE CLASSIFICAÇÃO

Art. 1º A classificação dos incidentes de segurança da informação será realizada pelo(a) Agente Responsável pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) ou por servidor(a) por ele(a) designado(a), com base na análise conjugada de seis dimensões de impacto, conforme os critérios estabelecidos nesta Instrução Normativa.

§1º Para fins de classificação dos incidentes, deverão ser consideradas as seguintes dimensões de impacto:

I — impacto na disponibilidade de serviços de tecnologia da informação e comunicação;

II — comprometimento de dados pessoais;

III — abrangência de usuários(as) afetados(as);

IV — repercussão institucional e jurídica;

V — sofisticação e persistência da ameaça; e

VI — complexidade de recuperação.

§2º A classificação inicial do incidente deverá ser realizada em até 30 (trinta) minutos após o registro do evento no sistema de gestão de incidentes, com base nas informações disponíveis naquele momento.

§3º O nível de severidade atribuído ao incidente corresponderá à dimensão de maior impacto identificada na avaliação, prevalecendo sempre o critério mais restritivo.

Art. 2º São critérios de classificação para o Nível 1 (Baixo):

I — **quanto à disponibilidade**: indisponibilidade de serviço não essencial ou degradação de desempenho que afete funcionalidade acessória, com duração estimada inferior a 1 (uma) hora e sem impacto na prestação jurisdicional;

II — **quanto a dados pessoais**: nenhum dado pessoal comprometido, exposto ou em risco de comprometimento;

III — **quanto à abrangência**: até 50 (cinquenta) usuários(as) internos(as) diretamente afetados(as), restritos a uma única unidade organizacional, sem afetar magistrados(as) ou serviços de atendimento ao público;

IV — **quanto à repercussão**: nenhuma repercussão institucional, midiática ou jurídica previsível;

V — **quanto à ameaça**: evento isolado, sem indícios de ação intencional ou coordenada, como falhas de configuração, mau uso de recursos, alertas de segurança de baixa confiança ou tentativas de ataque bloqueadas automaticamente pelas ferramentas de proteção;

VI — **quanto à recuperação**: resolução possível por meio de procedimentos operacionais padrão, sem necessidade de mobilização de áreas adicionais ou de restauração de backups.

Art. 3º São critérios de classificação para o Nível 2 (Médio):

I — **quanto à disponibilidade:** indisponibilidade parcial de serviço de apoio ou degradação significativa de desempenho em serviço essencial, com duração estimada entre 1 (uma) e 2 (duas) horas, podendo afetar a produtividade de unidades administrativas ou judiciárias sem interrupção completa da prestação jurisdicional;

II — **quanto a dados pessoais:** possibilidade de comprometimento de dados pessoais não sensíveis de até 500 (quinhentos) titulares, internos ou jurisdicionados, sem evidência de exfiltração confirmada;

III — **quanto à abrangência**: de 51 (cinquenta e um) a 500 (quinhentos) usuários(as) internos(as) diretamente afetados(as), podendo abranger mais de uma unidade organizacional, ou qualquer quantidade quando afetar magistrados(as) de uma única comarca ou unidade;

IV — **quanto à repercussão**: repercussão institucional limitada ao âmbito interno do Tribunal, sem potencial midiático externo identificado;

V — **quanto à ameaça:** possível ação intencional de baixa sofisticação, como infecção por malware comum em estação de trabalho isolada, phishing direcionado a poucos(as) usuários(as), acesso não autorizado a sistema não crítico ou vulnerabilidade explorada em componente de baixa criticidade;

VI — **quanto à recuperação**: resolução demandando atuação coordenada de mais de uma equipe técnica, podendo exigir aplicação de patches, restauração parcial de configurações ou isolamento temporário de ativos, com prazo estimado de recuperação de até 4 (quatro) horas.

Art. 4º São critérios de classificação para o Nível 3 (Alto):

I — **quanto à disponibilidade:** indisponibilidade total ou degradação severa de serviço essencial de TIC, incluindo sistemas judiciais (PJe, SEI, SAJECE), com duração estimada inferior a 2 (duas) horas ou que, embora inferior a esse limiar, afete diretamente a prestação jurisdicional em múltiplas unidades;

II — **quanto a dados pessoais:** comprometimento confirmado ou altamente provável de dados pessoais sensíveis em qualquer volume, ou de dados pessoais não sensíveis de mais de 500 (quinhentos) até 5.000 (cinco mil) titulares, ou comprometimento de dados jurisdicionais protegidos por sigilo (segredo de justiça, dados de menores, dados de vítimas), independentemente do volume;

III — **quanto à abrangência**: de 501 (quinhentos e um) a 2.500 (dois mil e quinhentos) usuários(as) internos(as) diretamente afetados(as), ou impacto em serviço utilizado por todas as unidades de uma comarca ou por uma diretoria inteira, ou qualquer quantidade quando afetar magistrados(as) de múltiplas comarcas;

IV — **quanto à repercussão:** repercussão institucional significativa, com potencial de questionamento por órgãos de controle (CNJ, ANPD, Ministério Público, Corregedoria), imprensa ou titulares de dados pessoais afetados;

V — **quanto à ameaça**: ação intencional de média a alta sofisticação, como ransomware em fase inicial de propagação sem cifragem massiva, comprometimento de conta de serviço com privilégios elevados, movimento lateral detectado na rede, exploração ativa de vulnerabilidade zero-day em componente de média criticidade, ou ataque de engenharia social bem-sucedido contra servidor(a) com acesso a informações restritas;

VI — **quanto à recuperação**: resolução demandando mobilização ampla de recursos técnicos e humanos, possível necessidade de restauração de backups, reconstrução parcial de ambientes, análise forense e envolvimento de prestadores de serviço especializados, com prazo estimado de recuperação superior a 4 (quatro) horas.

Art. 5º São critérios de classificação para o Nível 4 (Crítico), conforme definido no art. 9º, inciso IV, da Portaria nº 2303/2026, e detalhados a seguir:

I — **quanto à disponibilidade:** indisponibilidade total de serviço essencial de TIC por período igual ou superior a 2 (duas) horas, ou indisponibilidade simultânea de dois ou mais serviços essenciais por qualquer período, ou comprometimento do data center principal que ameace a continuidade global dos serviços;

II — **quanto a dados pessoais:** exfiltração confirmada de dados pessoais sensíveis de mais de 100 (cem) titulares, ou exfiltração confirmada de dados pessoais não sensíveis de mais de 5.000 (cinco mil) titulares, ou comprometimento de base de dados de sistema judicial estruturante (PJe, SAJECE) com potencial de exposição massiva de dados jurisdicionais;

III — **quanto à abrangência:** mais de 2.500 (dois mil e quinhentos) usuários(as) internos(as) diretamente afetados(as), ou mais de 25% (vinte e cinco por cento) da base de usuários(as), ou impacto generalizado que comprometa a capacidade de prestação jurisdicional em âmbito estadual;

IV — **quanto à repercussão:** repercussão institucional grave, com certeza ou alta probabilidade de exposição midiática, acionamento de órgãos de controle, obrigação de comunicação à ANPD nos termos do art. 48 da Lei nº 13.709/2018, possibilidade de danos morais ou patrimoniais a titulares, ou impacto na imagem e credibilidade do Poder Judiciário do Estado do Ceará;

V — **quanto à ameaça:** ataque cibernético coordenado ou persistente (APT), ransomware com cifragem massiva de dados ou sistemas, comprometimento de credenciais de administrador de domínio ou de sistemas críticos (PJe, Active Directory, controladores de domínio, hipervisores), comprometimento da cadeia de suprimentos, ataque destrutivo ou qualquer ameaça que indique atuação de agente com capacidade técnica avançada e objetivo deliberado de causar dano ao Tribunal;

VI — **quanto à recuperação:** resolução demandando ativação do Plano de Continuidade de Negócio e/ou do Plano de Recuperação de Desastres, possível necessidade de reconstrução integral de ambientes, contratação emergencial de serviços especializados, análise forense aprofundada e envolvimento de órgãos externos (CPTRIC-PJ, autoridades policiais, ANPD), com prazo de recuperação indeterminado ou superior a 24 (vinte e quatro) horas.

Art. 6º Constituem exemplos referenciais, não exaustivos, de incidentes típicos por nível de severidade:

I — **Nível 1 (Baixo):** alerta de antivírus em estação de trabalho/servidor isolada com ameaça automaticamente contida; tentativa de phishing reportada por usuário(a) sem clique no link malicioso; falha temporária em serviço de impressão; bloqueio de conta por excesso de tentativas de autenticação sem indícios de ataque; varredura de portas detectada e bloqueada pelo firewall; reinicialização não programada de servidor de baixa criticidade sem impacto em serviço; alerta de consumo anômalo de recursos em servidor/instância de nuvem sem evidência de comprometimento; falha de réplica entre nós de cluster em ambiente de homologação com correção automática;

II — **Nível 2 (Médio):** infecção por malware em estação de trabalho/servidor com potencial de propagação lateral ainda não confirmada; phishing com clique no link e possível coleta de credenciais de usuário(a) comum; indisponibilidade parcial de sistema administrativo não crítico; detecção de software não autorizado em servidor de baixa criticidade; acesso não autorizado a pasta de rede/nuvem compartilhada contendo dados pessoais não sensíveis; alerta de atividade suspeita em servidor de produção sem comprometimento confirmado; criação não autorizada de snapshot ou clone de máquina virtual; acesso indevido a console de gerenciamento de soluções/recursos de tecnologia/de nuvem com permissões limitadas (leitura) sem alteração de configuração; tentativa de escalação de privilégios em servidor/contêiner de aplicação sem impacto confirmado em outros serviços do host;

III — **Nível 3 (Alto):** ransomware detectado em fase inicial de propagação em segmento de rede; comprometimento de conta de serviço com acesso a banco de dados de sistema judicial/administrativo; indisponibilidade dos sistemas classificados como críticos; detecção de movimento lateral em rede interna/nuvem com comprometimento confirmado de mais de uma estação/um servidor; vazamento confirmado de dados pessoais sensíveis, conforme consideração da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados - LGPD, em volume restrito; exploração ativa de vulnerabilidade crítica em componente exposto à internet; comprometimento de servidor de produção com acesso a dados de sistemas judiciais/administrativos críticos; acesso não autorizado com permissões de escrita a console de gerenciamento de hipervisor ou de ambiente de nuvem; exfiltração de dados a partir de instância de nuvem ou de servidor on-premises contendo informações jurisdicionais;

IV — **Nível 4 (Crítico):** ransomware com cifragem ativa de servidores de produção; comprometimento de administrador de domínio do Active Directory; exfiltração massiva de dados jurisdicionais/usuários internos; indisponibilidade total do PJe em âmbito estadual; ataque destrutivo a infraestrutura virtualizada, incluindo hipervisores e plataformas de orquestração de contêineres; evidência de acesso persistente por agente

externo avançado; comprometimento de conta administrativa de provedor de nuvem com controle total sobre o tenant do Tribunal; destruição ou cifragem de backups armazenados em nuvem ou em ambiente off-site, comprometendo a capacidade de recuperação.

CAPÍTULO II

DA RECLASSIFICAÇÃO

Art. 7º O nível de severidade atribuído a um incidente poderá ser reclassificado a qualquer tempo durante o seu ciclo de vida, com base em novas informações obtidas no curso da investigação e do tratamento.

§1º A reclassificação para nível superior será realizada pelo(a) Agente Responsável pela ETIR ou pelo(a) Coordenador(a) Estratégico(a), devendo ser registrada no sistema de gestão de incidentes com a justificativa correspondente e implicando a adoção imediata dos procedimentos de escalonamento e comunicação do novo nível.

§2º A reclassificação para nível inferior somente será realizada após confirmação de que os critérios do nível originalmente atribuído não se verificam, devendo igualmente ser registrada com justificativa.

§3º A elevação de qualquer incidente ao Nível 4 (Crítico) deverá ser comunicada ao(à) Coordenador(a) Estratégico(a) de forma imediata, por meio de contato direto (ligação telefônica, mensagem instantânea ou presencialmente), independentemente do horário.

CAPÍTULO III

DOS PROCEDIMENTOS DE ESCALONAMENTO

Art. 8º O escalonamento de incidentes de segurança da informação observará a seguinte cadeia funcional:

I — primeiro nível de escalonamento: do(a) servidor(a) ou equipe técnica que detectou o evento para o(a) agente responsável pela ETIR ou para o(a) Gerente de Cibersegurança e Ambientes Tecnológicos;

II — segundo nível de escalonamento: do(a) Agente Responsável para o(a) Coordenador(a) Estratégico(a) da ETIR;

III — terceiro nível de escalonamento: do(a) Coordenador(a) Estratégico(a) para o CGSICCPDP e para a Presidência;

IV — quarto nível de escalonamento: do CGSICCPDP para órgãos externos (CPTRIC-PJ, ANPD, autoridades policiais), conforme a natureza do incidente.

Art. 9º Os prazos máximos para escalonamento de incidentes de segurança da informação, contados a partir da detecção ou do recebimento da notificação, são:

I — **Nível 1 (Baixo)**:

a) registro no sistema de gestão de incidentes em até 2 (duas) horas;

b) comunicação ao(à) agente responsável em até 4 (quatro) horas, podendo ser realizada por meio do próprio sistema de gestão ou por correio eletrônico; e

c) sem escalonamento adicional obrigatório;

II — **Nível 2 (Médio):**

a) registro no sistema de gestão de incidentes em até 1 (uma) hora;

b) comunicação ao(à) agente responsável em até 1 (uma) hora; comunicação ao(à) Coordenador(a) Estratégico(a) em até 2 (duas) horas quando o incidente envolver dados pessoais; e

c) mobilização das áreas técnicas pertinentes em até 2 (duas) horas;

III — **Nível 3 (Alto):**

a) registro imediato no sistema de gestão de incidentes;

b) comunicação imediata ao(à) agente responsável por contato direto;

c) comunicação ao(à) Coordenador(a) Estratégico(a) em até 30 (trinta) minutos;

d) comunicação ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais em até 1 (uma) hora quando envolver dados pessoais;

e) reporte ao CPTRIC-PJ em até 2 (duas) horas; e

f) comunicação à Alta Administração em até 2 (duas) horas;

IV — **Nível 4 (Crítico):**

a) registro imediato no sistema de gestão de incidentes;

b) comunicação imediata ao(à) agente responsável e ao(à) Coordenador(a) Estratégico(a) por contato direto, independentemente do horário;

c) acionamento do CGSICCPDP em até 30 (trinta) minutos pelo(a) Coordenador(a) Estratégico(a);

d) comunicação à Presidência em até 30 (trinta) minutos;

e) comunicação ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais em até 1 (uma) hora quando envolver dados pessoais; e

f) reporte ao CPTRIC-PJ em até 1 (uma) hora.

§1º Os prazos previstos neste artigo são contados em horas corridas, incluindo horários fora do expediente,

finais de semana e feriados, quando o incidente for classificado nos Níveis 3 (Alto) ou 4 (Crítico).

§2º Para incidentes dos Níveis 1 (Baixo) e 2 (Médio), os prazos são contados em horas úteis, salvo quando houver risco iminente de agravamento.

Art. 10. Para os fins desta Instrução Normativa, considera-se comunicação imediata aquela realizada sem qualquer atraso deliberado, tão logo o(a) responsável pelo escalonamento tenha condições de efetuar o contato, utilizando preferencialmente contato direto por telefone, mensagem instantânea ou comunicação presencial.

Art. 11. O(A) Agente Responsável pela ETIR manterá atualizada lista de contatos de emergência contendo, no mínimo:

I — nome, telefone celular, correio eletrônico e aplicativo de mensagens instantâneas de todos(as) os(as) integrantes do Núcleo Estratégico e Decisório;

II — nome e contato do(a) Encarregado(a) pelo Tratamento de Dados Pessoais e de seu(sua) substituto(a);

III — contatos dos(as) integrantes do Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais (CGSICCPDP);

IV — contatos dos prestadores de serviço de segurança com contrato vigente; e

V — contatos de órgãos de segurança pública especializados em crimes cibernéticos.

Parágrafo único. A lista de contatos será revisada trimestralmente e após qualquer alteração na composição da ETIR ou do CGSICCPDP.

CAPÍTULO IV

DOS PROCEDIMENTOS DE COMUNICAÇÃO

SEÇÃO I

Da Comunicação Interna

Art. 12. Para incidentes de Nível 1 (Baixo), a comunicação interna limitar-se-á ao registro no sistema de gestão de incidentes e à ciência do(a) Agente Responsável, dispensadas comunicações adicionais salvo solicitação expressa.

Art. 13. Para incidentes de Nível 2 (Médio), além do registro no sistema de gestão de incidentes, serão realizadas as seguintes comunicações internas:

I — comunicação ao(à) Agente Responsável pela ETIR, contendo a descrição do evento, a classificação atribuída, os ativos afetados e as ações iniciais adotadas;

II — comunicação aos(às) integrantes do Núcleo Estratégico e Decisório cujas áreas estejam diretamente

envolvidas no incidente;

III — quando o incidente envolver dados pessoais, comunicação ao(à) Coordenador(a) Estratégico(a), que avaliará a necessidade de acionamento do(a) Encarregado(a) pelo Tratamento de Dados Pessoais;

IV — comunicação de encerramento ao(à) agente responsável, com resumo das ações adotadas e do resultado alcançado.

Art. 14. Para incidentes de Nível 3 (Alto), além das providências previstas no artigo anterior, serão realizadas as seguintes comunicações internas:

I — comunicação imediata ao(à) Coordenador(a) Estratégico(a), contendo a descrição do incidente, a classificação, a avaliação preliminar de impacto e as ações de contenção em curso;

II — comunicação ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais quando o incidente envolver dados pessoais, contendo a natureza dos dados possivelmente comprometidos, o volume estimado de titulares afetados(as) e as medidas adotadas para mitigar o impacto;

III — comunicação à Alta Administração pelo(a) Coordenador(a) Estratégico(a), informando a natureza do incidente, o impacto nos serviços e as medidas em curso;

IV — atualizações periódicas ao(à) Coordenador(a) Estratégico(a) a cada 2 (duas) horas ou sempre que houver mudança relevante no cenário, enquanto o incidente estiver em curso;

V — comunicação de encerramento ao(à) Coordenador(a) Estratégico(a) e à Alta Administração, acompanhada do Relatório de Comunicação de Incidente de Segurança previsto no art. 23 da Portaria nº 2303/2026.

Art. 15. Para incidentes de Nível 4 (Crítico), além das providências previstas nos artigos anteriores, serão realizadas as seguintes comunicações internas:

I — acionamento imediato do CGSICCPDP pelo(a) Coordenador(a) Estratégico(a), com convocação de reunião emergencial presencial ou por videoconferência;

II — comunicação imediata à Presidência do Tribunal pelo(a) Coordenador(a) Estratégico(a);

III — comunicação a todos(as) os(as) integrantes do Núcleo Estratégico e Decisório, com convocação para atuação imediata, independentemente do horário;

IV — acionamento dos(as) integrantes do Grupo de Apoio Técnico Especializado pertinentes à tipologia do incidente;

V — atualizações ao CGSICCPDP e à Presidência a cada 1 (uma) hora ou sempre que houver mudança relevante no cenário;

VI — quando o impacto afetar a prestação jurisdicional, comunicação à Corregedoria-Geral de Justiça pelo(a) Coordenador(a) Estratégico(a), informando a natureza do incidente e a previsão de restabelecimento;

VII — quando o impacto afetar os serviços prestados ao público externo, comunicação à Assessoria de

Comunicação (ASCOM) pelo(a) Coordenador(a) Estratégico(a), subsidiando a eventual necessidade de pronunciamento público.

SEÇÃO II

Da Comunicação Externa

Art. 16. A comunicação externa decorrente de incidentes de segurança da informação é de competência exclusiva do(a) Coordenador(a) Estratégico(a) da ETIR, ou do CGSICCPDP nos casos de incidentes críticos, vedada a comunicação direta por outros(as) integrantes da ETIR a órgãos externos, imprensa ou público em geral, salvo delegação expressa.

Art. 17. O reporte ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) será obrigatório para incidentes classificados nos Níveis 3 (Alto) e 4 (Crítico) e deverá ser realizado pelo(a) Coordenador(a) Estratégico(a) da ETIR nos prazos previstos no art. 9º desta Instrução Normativa, contendo as informações mínimas exigidas pelos protocolos do Conselho Nacional de Justiça.

Art. 18. A comunicação à Autoridade Nacional de Proteção de Dados (ANPD) será realizada nos termos do art. 48 da Lei nº 13.709/2018 e da regulamentação própria da ANPD.

§1º A avaliação preliminar sobre a necessidade de comunicação à ANDP será realizada conjuntamente pelo(a) Coordenador(a) Estratégico(a) e pelo(a) Encarregado(a) pelo Tratamento de Dados Pessoais, no prazo máximo de 24 (vinte e quatro) horas após a confirmação do comprometimento de dados pessoais;

§2º A comunicação à ANPD, quando devida, será formalizada pelo(a) Encarregado(a) pelo Tratamento de Dados Pessoais, com subsídios técnicos fornecidos pela ETIR, no prazo estabelecido pela regulamentação da ANPD;

§3º A comunicação aos(às) titulares afetados(as), quando devida, será coordenada pelo(a) Encarregado(a) pelo Tratamento de Dados Pessoais em articulação com a ASCOM, observando-se clareza, objetividade e linguagem acessível.

Art. 19. A comunicação a órgãos de segurança pública será realizada pelo CGSICCPDP, com anuência da Presidência, sempre que houver indícios de prática criminosa, em especial nos casos de:

I — invasão de dispositivo informático (art. 154-A do Código Penal);

II — interrupção ou perturbação de serviço informático (art. 266 do Código Penal);

III — inserção de dados falsos em sistema de informações (art. 313-A do Código Penal);

IV — modificação ou alteração não autorizada de sistema de informações (art. 313-B do Código Penal);

V — extorsão mediante ameaça de divulgação de dados ou de manutenção de cifragem (ransomware);

VI — outros ilícitos cibernéticos identificados no curso da investigação do incidente.

SEÇÃO III

Da Comunicação ao Público e à Imprensa

Art. 20. A comunicação pública sobre incidentes de segurança da informação será de competência exclusiva da Presidência do Tribunal ou de quem ela designar, com apoio técnico da DSI e operacionalização pela ASCOM.

§1º O(A) Coordenador(a) Estratégico(a) fornecerá à ASCOM informações técnicas em linguagem acessível para subsidiar a elaboração de notas, comunicados ou respostas a veículos de imprensa.

§2º Nenhum(a) integrante da ETIR se manifestará publicamente, em nome pessoal ou do Tribunal, sobre incidentes em curso, inclusive em redes sociais.

CAPÍTULO V

DA DOCUMENTAÇÃO E DOS REGISTROS

Art. 21. Todos os incidentes, independentemente do nível de severidade, serão registrados no sistema de gestão de incidentes, contendo, no mínimo:

I — identificação única do incidente (número sequencial);

II — data e hora da detecção;

III — data e hora do registro;

IV — fonte da notificação (monitoramento automatizado, relato de usuário(a), alerta externo);

V — descrição do evento;

VI — classificação de severidade (inicial e reclassificações, se houver);

VII — ativos afetados;

VIII — ações de contenção, erradicação e recuperação adotadas;

IX — registros de escalonamento e comunicações realizadas, com data, hora e destinatário;

X — data e hora do encerramento;

XI — responsável pelo tratamento;

XII — lições aprendidas e recomendações (obrigatório para Níveis 3 e 4, facultativo para Níveis 1 e 2).

Art. 22. Para incidentes de Níveis 3 (Alto) e 4 (Crítico), além do registro no sistema, serão elaborados o Relatório de Comunicação de Incidente de Segurança e o Termo de Custódia dos Ativos de Informação previstos no art. 23 da Portaria nº 2303/2026.

§1º O Relatório de Comunicação de Incidente de Segurança será elaborado pelo(a) Agente Responsável pela ETIR e submetido ao(à) Coordenador(a) Estratégico(a) no prazo de 5 (cinco) dias úteis após o encerramento do incidente.

§2º Para incidentes de Nível 4 (Crítico), o relatório será complementado por análise de causa-raiz e por plano de ação com medidas corretivas e preventivas, com responsáveis e prazos, a ser submetido ao CGSICCPDP no prazo de 15 (quinze) dias úteis após o encerramento do incidente.

CAPÍTULO VI

DOS HORÁRIOS E DA DISPONIBILIDADE

Art. 23. Para incidentes de Nível 1 (Baixo) e 2 (Médio), os procedimentos de escalonamento e comunicação serão executados durante o horário de expediente regular do Tribunal.

Parágrafo único. Quando um incidente de Nível 1 (Baixo) ou 2 (Médio) for detectado fora do horário de expediente por ferramentas de monitoramento automatizado, o registro será realizado automaticamente pela ferramenta e o escalonamento será executado no primeiro horário útil subsequente, salvo se houver indicativos de agravamento que justifiquem a reclassificação.

Art. 24. Para incidentes de Nível 3 (Alto) e 4 (Crítico), os procedimentos de escalonamento e comunicação serão executados em regime ininterrupto, independentemente de horário, dia da semana ou feriado.

Parágrafo único. O(A) Agente Responsável pela ETIR assegurará que os meios de contato de emergência previstos no art. 11 desta Instrução Normativa estejam acessíveis e operacionais permanentemente.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 25. Os prazos e procedimentos estabelecidos nesta Instrução Normativa poderão ser adaptados pelo(a) Agente Responsável pela ETIR durante o tratamento de um incidente específico, mediante justificativa registrada no sistema de gestão de incidentes, quando circunstâncias excepcionais assim o exigirem.

Art. 26. Os modelos padronizados dos documentos referidos nesta Instrução Normativa (Relatório de Comunicação de Incidente de Segurança, Termo de Custódia dos Ativos de Informação e formulário de reporte ao CPTRIC-PJ) constam como anexo neste ato.

Art. 27. Esta Instrução Normativa será revisada sempre que houver alteração nos protocolos do CNJ, na composição da ETIR ou nos procedimentos nela estabelecidos, e, em qualquer caso, em prazo não superior a 24 (vinte e quatro) meses contados da publicação ou da última revisão.

Art. 28. Esta Instrução Normativa entra em vigor na data de sua publicação.

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

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, em Fortaleza, aos 29 (vinte e nove) dias de setembro de 2026.

Desembargador Heráclito Vieira de Sousa Neto
Presidente do Tribunal de Justiça do Estado do Ceará

ANEXO I - MODELO A – RELATÓRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA CIBERNÉTICA

TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ - ETIR

DADOS DE CONTROLE

Nº da ocorrência/ano:	
Nível de severidade:	( )Crítica ( )Alta ( )Média ( )Baixa
Data/hora da detecção:	/ / às : (HLB)
Data de elaboração:	/ /

1. **RESPONSÁVEL PELA PRESERVAÇÃO DOS DADOS**

Nome:	

Matrícula:	
Unidade organizacional:	
Endereço eletrônico:	
Telefone:	

2. **RESPONSÁVEL PELA ETIR**

Endereço eletrônico:	
Matrícula:	
Nome:	
Telefone:	
Unidade organizacional:	

3. **ÓRGÃO COMUNICANTE**

Órgão:	

Endereço:	

4. **CATEGORIA DO INCIDENTE**

( ) Campanha de phishing

( ) Degradação ou interrupção de serviços (DoS/DDoS)

( ) Comprometimento de credenciais com acesso a informações sensíveis

( ) Impossibilidade de acesso à informação por encriptação (ransomware)

( ) Vazamento de informação e/ou dados pessoais

( ) Acesso não autorizado a sistemas ou bases de dados

( ) Desfiguração de página eletrônica (defacement)

( ) Malware / código malicioso

( ) Exploração de vulnerabilidade

( ) Outro: _____

5. **RELATO SOBRE O INCIDENTE**

DESCREVA O INCIDENTE:

_____
_____
_____

ORIGEM DO INCIDENTE (ou razão pela qual não foi possível identificá-la):

_____
_____
_____

COMO FOI DETECTADO O INCIDENTE?

_____
_____
_____

QUAL O IMPACTO IDENTIFICADO (disponibilidade, integridade, confidencialidade, autenticidade)?

_____
_____

_____

QUAIS FORAM OS DADOS COLETADOS E PRESERVADOS?

_____

_____

_____

6. **DADOS PESSOAIS ENVOLVIDOS**

O incidente envolveu dados pessoais? ( ) Sim ( ) Não

Natureza dos dados (comuns / sensíveis / crianças e adolescentes): _____

Quantidade estimada de titulares afetados: _____

O Encarregado de Dados Pessoais foi comunicado? ( ) Sim ( ) Não

Necessidade de comunicação à ANPD (art. 48, LGPD)? ( ) Sim ( ) Não ( ) Em análise

7. **AÇÕES DE TRATAMENTO E RESPOSTA**

QUAIS FORAM AS AÇÕES DE TRATAMENTO E RESPOSTA AO INCIDENTE?

_____

_____

_____

COMO FORAM PRESERVADOS OS REGISTROS? QUAIS AS FERRAMENTAS UTILIZADAS?

_____

_____

_____

QUAL FOI O LOCAL DE ARMAZENAMENTO DAS INFORMAÇÕES PRESERVADAS?

_____

_____

_____

8. **RESUMO CRIPTOGRÁFICO**

Algoritmo utilizado (ex.: SHA-256): _____

Resumo criptográfico do arquivo contendo a lista de hashes:

_____

_____

_____

A lista completa dos resumos criptográficos encontra-se em anexo.

9. **MATERIAL CUSTODIADO**

Termo de Custódia: ( ) Anexo ( ) Não aplicável

Nº de lacre de material físico preservado: _____

10. **INVIABILIDADE DE PRESERVAÇÃO DE MÍDIAS**

( ) Não aplicável – mídias preservadas integralmente

( ) Aplicável – justificativa abaixo:

_____
_____
_____

11. **COMUNICAÇÕES REALIZADAS**

Destinatário	Comunicado?	Data
Presidência do TJCE	( ) Sim ( ) Não	___/___/_____
CPTRIC-PJ (CNJ)	( ) Sim ( ) Não	___/___/_____
Ministério Público	( ) Sim ( ) Não	___/___/_____
Órgão de Polícia Judiciária	( ) Sim ( ) Não	___/___/_____
Encarregado de Dados Pessoais	( ) Sim ( ) Não	___/___/_____
ANPD (se aplicável)	( ) Sim ( ) Não	___/___/_____

Comitê de Crise (se aplicável)	( ) Sim ( ) Não	___/___/_____

12. **OUTROS DADOS JULGADOS RELEVANTES**

_____
_____
_____

Local e data: _____, _____ /____ /_____

_____

Assinatura do agente responsável pela preservação dos dados do incidente

_____

Assinatura do agente responsável pela ETIR

MODELO B – TERMO DE CUSTÓDIA DOS ATIVOS DE INFORMAÇÃO RELACIONADOS AO INCIDENTE DE SEGURANÇA

TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ - ETIR

DADOS DE CONTROLE

Nº da ocorrência/ano:	(vinculado ao Relatório de Comunicação)
Data de preenchimento:	___/___/_____

DADOS DO CUSTODIANTE

Nome:	

Matrícula:	
Órgão:	
Unidade organizacional:	
Cargo/Função:	
Endereço:	
Telefone:	
Endereço eletrônico:	

LOCAL DE ARMAZENAMENTO

Endereço/descrição do local: _____
_____
_____

Condições de acesso (controle físico, chave, biometria): _____
_____
_____

MATERIAIS SOB CUSTÓDIA

ITEM	TIPO	QTDE	DESCRIÇÃO	IDENTIF./LACRE	HASH

CADEIA DE CUSTÓDIA

Seq.	Data/Hora	Ação	De	Para	Motivo

Local e data: _____, _____ /____ /_____

_____

Custodiante

_____

Agente responsável pela ETIR

Atenção! Essa matéria possui outra(s) vinculada(s) a ela. Para ver as mudanças siga as instruções abaixo.

Para visualizar a matéria completa, acesse o link https://djea-con.tjce.jus.br/materias/179942 ou realize a leitura do QR-Code ao lado.