juiz.especiais@tjce.jus.br, no prazo de 2 (dois) dias úteis contados da publicação desta Portaria.

§2º O descumprimento do disposto no §1º será considerado desistência e implicará eliminação do Programa de Juízes(as) Leigos(as) do Tribunal de Justiça do Estado do Ceará.

Art. 3º Esta Portaria entrará 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, aos 12 dias do mês de julho de 2022.

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

ANEXO I
JUÍZES(AS) LEIGOS(AS) - DESISTÊNCIA

Inscrição	Nome	Ato de Designação
922001741	Renan Melo Aragão Timbó Martins Mendes Furtado	Portaria nº 1541/2022
922001442	Camila Rodolfo de Sá Batista	Portaria nº 1560/2022

ANEXO II
DESIGNAÇÃO DEJUÍZES(AS) LEIGOS (AS)

Inscrição	Nome	Classif. Geral	Origem da Vaga	Unidade de Lotação
922002536	John Gledyson Araujo Vieira	378ª	Art. 1º desta Portaria	1ª Unidade de Juizado Especial Cível da Comarca de Fortaleza
922002861	Christianne Marques Meirelles	360ª	Art. 1º desta Portaria	1ª Turma Recursal vinculada ao Juiz de Direito Antônio Alves Araújo

PORTARIA Nº 1592/2022

Dispõe sobre a revogação parcial da Portaria n° 1574/2022 e designação do Juiz de Direito Francisco Biserril Azevedo de Queiroz.

A Presidente do Tribunal de Justiça do Estado do Ceará, no uso de suas atribuições legais, ao apreciar o Processo Administrativo n° 8500459-94.2022.8.06.0064;

RESOLVE revogar parcialmente a Portaria n° 1574/2022, na parte que designou a Juíza de Direito Elizabete Silva Pinheiro, para, sem prejuízo de suas funções, auxiliar o 4º Núcleo Regional de Custódia e de Inquérito da Comarca de Caucaia, e designar o Juiz de Direito Francisco Biserril Azevedo de Queiroz, Titular da 2ª Vara Cível da Comarca de Caucaia, para auxiliar a referida Unidade, durante licença do magistrado David Ribeiro de Souza Belém, no período de 11 de julho a 15 de julho de 2022.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, Fortaleza, 12 de julho de 2022.

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

PORTARIA Nº 1593/2022

Aprova a Norma Geral para Cópias de Segurança da Informação (*Backup*) no âmbito do Poder Judiciário do Estado do Ceará.

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

CONSIDERANDO os termos da Resolução do Conselho Nacional de Justiça (CNJ) n° 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e estabeleceu as diretrizes para sua governança, gestão e infraestrutura;

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 Resolução do Órgão Especial do TJCE n° 25/2016, que regulamenta a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Ceará;

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); e

CONSIDERANDO as boas práticas de Governança de 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 a Norma Geral para Cópias de Segurança da Informação (*Backup*), que tem por objetivo definir as diretrizes gerais e as responsabilidades para a execução de cópias de segurança (*backup*) no âmbito do Poder Judiciário do Estado do Ceará, na forma do Anexo I desta Portaria.

Art. 2º A Secretaria de Tecnologia da Informação deverá informar ao Comitê de Governança de Segurança da Informação e de Crises Cibernéticas, em até 90 (noventa) dias após publicação deste ato, o tempo necessário para adequar-se aos itens deste normativo.

Art. 3º Os casos não previstos deverão ser apreciados pelo Comitê de Governança de Segurança da Informação e de Crises Cibernéticas.

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

REGISTRE-SE, PUBLIQUE-SE E CUMPRA-SE.
GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, em Fortaleza, aos 12 de julho de 2022.

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

ANEXO I DA PORTARIA Nº 1593/2022

NORMA GERAL PARA CÓPIAS DE SEGURANÇA (*BACKUP*)

Art. 1º Objetivo: normatizar a política de cópias de segurança (*backup*) no âmbito do Poder Judiciário do Estado do Ceará.
Art. 2º Abrangência: esta norma se aplica a todas as soluções tecnológicas utilizadas e mantidas no âmbito do Poder Judiciário do Estado do Ceará.
Art. 3º Termos e definições:
I - usuário(a): magistrados(as) e servidores(as) ocupantes de cargo efetivo ou em comissão, requisitados(as) e cedidos(as), desde que previamente autorizados(as), empregados(as) de empresas prestadoras de serviços terceirizados, conveniados(as), consultores(as), estagiários(as), e outras pessoas que se encontrem a serviço da Justiça Estadual, utilizando em caráter temporário os recursos tecnológicos do Poder Judiciário do Estado do Ceará;
II - segurança da informação: proteção da informação contra ameaças para garantir a continuidade do negócio, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio, preservando a confidencialidade, a integridade e a disponibilidade da informação;
III - cópias de segurança (*backup*): cópia de segurança de dados computacionais, que pode ser utilizada ou consultada após sua restauração em caso de indisponibilidade, perda ou alteração dos dados originais;
IV - integridade: garantia de que a informação seja mantida em seu estado original, visando a protegê-la, na guarda ou na transmissão, contra alterações indevidas, intencionais ou acidentais;
V - confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas; e
VI - disponibilidade: garantia de que os(as) usuários(as) autorizados(as) obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
Art. 4º Diretrizes:
I - garantir que todos os dados dos sistemas tenham cópias de segurança (*backups*), realizadas automaticamente e de forma regular;
II - garantir que todos os sistemas chave da organização tenham suas cópias de segurança (*backups*) realizadas como um sistema completo, por meio de processos como a geração de imagem, de forma a permitir uma rápida recuperação de todo o sistema;
III - testar a integridade dos dados nas mídias das cópias de segurança de forma regular, por meio da realização de um processo de restauração dos dados, de forma a garantir que o processo de cópia de segurança (*backup*) esteja sendo executado de forma apropriada;
IV - garantir que as cópias de segurança (*backups*) sejam apropriadamente protegidas por meio de segurança física ou criptografia quando forem armazenadas ou quando forem movimentadas através da rede, incluindo cópias de segurança (*backups*) remotas e em serviços de nuvem;
V - garantir que todas as cópias de segurança contenham ao menos uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional;
VI - o Poder Judiciário do Estado do Ceará, através da Gerência de Infraestrutura de Tecnologia da Informação, deverá realizar cópias de segurança (*backup*) de informações, softwares, imagens, áudios e vídeos, as quais deverão ser efetuadas e testadas regularmente conforme a geração de cópias de segurança definida nesta norma e em seus procedimentos;
VII - no que diz respeito à realização de cópias de segurança (*backup*), serão de responsabilidade da área de Tecnologia da Informação do Poder Judiciário do Estado Ceará somente os dados corporativos armazenados no *data center* ou em soluções em nuvem mantidas pela área de Tecnologia da Informação; os *backups* de dados/arquivos das máquinas dos(as) usuários(as) serão de responsabilidade do(a) próprio(a) usuário(a);
VIII - de preferência, as cópias de segurança deverão ser realizadas por meio de *softwares* corporativos que permitam manter e gerenciar as cópias de segurança dos arquivos e conteúdo de bases de dados, garantindo a disponibilidade e a acessibilidade das cópias feitas para propósitos de recuperação e para armazenamento de longo prazo;
IX - todo *backup* deve ser classificado com atributos: permissão de acesso, data, tempo de retenção, local de armazenamento, prioridade de recuperação dos dados;
X - o tempo de retenção padrão para os *backups* (diário, semanal, mensal e anual) deve ser o estabelecido na Tabela de Temporalidade de Documentos Administrativos do Poder Judiciário do Estado do Ceará (TTDA), devendo ser aplicado a todos

os tipos de cópias de segurança das soluções tecnológicas classificadas neste normativo e devem atender ao especificado nos itens abaixo:

a) caberá ao(à) gestor(a) do sistema definir os tempos de retenções que sejam diversos do padrão definido na Tabela de Temporalidade;

b) expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização e número de leitura/gravação; a fita não deverá ultrapassar 30 (trinta) anos de armazenamento, devendo ser copiada para outra mídia, destruída e descartada em lugar destinado para tal, obedecendo-se às leis ambientais; e

c) o(a) gestor(a) do sistema ou da informação poderá definir o tempo de retenção de acordo com normativos específicos; o(a) gestor(a) do sistema ou da informação deverá comunicar formalmente, através de processo administrativo encaminhado à Secretaria de Tecnologia da Informação, sempre que for necessário definir período de retenção das cópias de segurança superior ao definido nesta norma;

XI - deve-se categorizar os dados baseando-se na prioridade de recuperação;

XII - utilizar *backup* incremental e completo;

XIII - a Gerência de Infraestrutura de Tecnologia da Informação deverá assegurar-se de que a largura de banda da rede e o subsistema do disco sejam capazes de suportar uma quantidade grande de dados, tais como a recuperação do *backup* completo; caso exista algum impedimento técnico que impossibilite a execução da política de *backup* definida, a Gerência de Infraestrutura de Tecnologia da Informação deverá encaminhar, através de processo administrativo, parecer técnico detalhado, descrevendo os motivos, as ações para correção e as demais informações para decisão da administração superior, que poderá realizar novos investimentos para suprir possíveis deficiências ou aceitar uma nova política de *backup*;

XIV - o *backup* deve ser agendado de forma a não interferir nas atividades administrativas e judiciais;

XV - deverá haver ações proativas dos processos automatizados através da ferramenta de *backup* para assegurar, manter e recuperar o *backup*;

XVI - os volumes dos *backups* das aplicações devem ser separados de arquivos de dados e de arquivos de registros;

XVII - para a recuperação dos dados, os procedimentos de recuperação devem ser testados periodicamente, de acordo com a política de *backup* do Poder Judiciário do Estado do Ceará ou quando requisitado pelo(a) Secretário(a) de Tecnologia da Informação ou do Comitê de Governança de Segurança da Informação e de Crises Cibernéticas;

XVIII - em relação ao local onde é guardado o *backup* realizado nas instalações do Poder Judiciário do Estado do Ceará:

a) deve ser restrito;

b) deve ser protegido contra agentes naturais prejudiciais aos dados ou aos recursos computacionais;

c) todas as cópias (*backup*) devem ser armazenadas em ambientes providos pelo Poder Judiciário do Estado do Ceará;

d) as cópias de segurança deverão ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal; e

e) em situações onde a confidencialidade é importante, cópias de segurança deverão ser protegidas através de encriptação;

XIX - em relação aos *backups* realizados através de soluções disponibilizadas em nuvem ou *backups* em nuvem, em ambiente fora das instalações do Poder Judiciário do Estado do Ceará:

a) a responsabilidade pelo *backup* será da prestadora de serviços, assegurado um prazo de retenção definido em cláusulas contratuais; e

b) a política de *backup* a ser adotada deverá ser definida pela equipe de contratação da solução em nuvem ou solução de *backup* em nuvem e deverá atender aos requisitos da área de negócio para o tipo de dados/informações/arquivos que serão armazenados;

XX - deverá ser designado um(a) responsável por todo o processo de transporte e guarda das mídias de dados geradas no ambiente do Poder Judiciário do Estado do Ceará, devendo ser considerado o seguinte:

a) haver, para transporte de um local físico para outro, escolta com policiais da Assistência Militar, principalmente quando se tratar de mídias com informações sensíveis;

b) criptografar os dados do *backup*;

c) saber exatamente quem faz a manipulação dos dados sensíveis quando chegam às instalações de armazenamento; e

d) haver uma fiscalização do pessoal responsável pela guarda dos dados, devendo-se exigir garantia de segurança junto à empresa que faz o transporte e o armazenamento;

XXI - arquivos, se gravados apenas localmente nos computadores/*notebooks* corporativos (por exemplo, no *"drive C:"*), não terão garantia de *backup* e poderão ser perdidos caso ocorra uma falha no computador/*notebook* corporativo, sendo, portanto, de responsabilidade do(a) próprio(a) usuário(a);

XXII - será de responsabilidade do Poder Judiciário do Estado do Ceará prover todas as mídias para os *backups* realizados através dos equipamentos instalados em suas dependências; e

XXIII - devem ser realizadas cópias de segurança (*backups*) para as seguintes soluções tecnológicas:

a) sistemas Judicias e Administrativos (SJSA);

b) bases de dados dos Sistemas Judicias e Administrativos (BDSJSA);

c) gravações telefônicas e outras ferramentas multicanais (*ominichannel*) das Centrais de Atendimento (GTFMCA);

d) todos os áudios e os vídeos relativos às audiências do processo eletrônico (AVPE);

e) áudios e vídeos de processos não eletrônicos, quando solicitado pelo(a) juiz(juíza) diretor(a) do Fórum ou juizado (AVNPE);

f) arquivos e pastas dos servidores de rede e Sistemas de Arquivos (APSA);

g) *e-mails* dos usuários e seus respectivos anexos que possuam conta no domínio tjce.jus.br (E-MAIL);

h) eventos (*logs*) das soluções de segurança, auditoria e acessos de toda as soluções mantidas pela Secretaria de Tecnologia da Informação e pela Gerência de Informática do Fórum Clóvis Beviláqua, de acordo com a legislação em vigor e as resoluções do Conselho Nacional de Justiça (LOGS); e

i) outras soluções autorizadas pelo(a) Secretário(a) de Tecnologia da Informação.

Art. 5° Competências e responsabilidades:

I - dos(as) usuários(as) e colaboradores(as):

a) utilizar e manusear corretamente os recursos computacionais sob sua responsabilidade para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pela Secretaria de Tecnologia da Informação e a Gerência de Informática do Fórum Clóvis Beviláqua;

b) manter a configuração do equipamento disponibilizado pelo Poder Judiciário do Estado do Ceará, seguindo os devidos controles de segurança exigidos pelas normas específicas da instituição, assumindo a responsabilidade como custodiante das informações;

c) solicitar à área de Tecnologia da Informação a realização de cópias de segurança em equipamentos corporativos, desde que os dados e as informações sejam para uso institucional; e

d) conhecer o conteúdo e contribuir para a execução e o cumprimento desta norma;

II - da Assistência Militar:

a) diligenciar, dentro de sua competência, as eventuais ocorrências de furto, roubo ou extravio de componentes ou de recursos computacionais (*hardware* e *software*) relativos às mídias usadas para realizar cópias de segurança (*backup*) no âmbito do Poder Judiciário do Estado do Ceará após requisição feita às Presidências da Comissão de Segurança Permanente e/ou do Tribunal de Justiça do Estado do Ceará mediante solicitação dos(as) Secretários(as) das áreas de Tecnologia da Informação, Infraestrutura e Administração, dos(as) Diretores(as) de Fóruns e órgãos;

b) controlar, de acordo com processos definidos e dentro de sua competência, o acesso físico aos locais onde são armazenadas as cópias de segurança do Poder Judiciário do Estado do Ceará;

c) diligenciar, dentro de sua competência, acessos físicos não autorizados a ambientes críticos de Tecnologia da Informação, como os *data centers* e os locais onde são hospedados os *racks* e as fibras óticas e armazenadas as cópias de segurança; e

d) monitorar, ininterruptamente, o local (interno e externo) onde são armazenadas as cópias de segurança do Poder Judiciário do Estado do Ceará, utilizando, no mínimo, sistema de cftv, armazenamento de sistema de cftv e controle biométrico;

III - da Secretaria de Administração e Infraestrutura:

a) definir, construir e manter ambientes adequados para a guarda de cópias de segurança (*backup*);

b) garantir que os ambientes sejam protegidos contra agentes naturais prejudiciais aos dados ou aos recursos computacionais;

c) quando solicitado pela Secretaria de Tecnologia da Informação, designar um(a) responsável pelo transporte das mídias de dados; este serviço deverá ser acompanhado por servidor(a) da Infraestrutura de Tecnologia da Informação;

d) garantir, com o apoio da Assistência Militar, o transporte de um local físico para outro, principalmente quando se tratar de mídias com informações sensíveis;

e) manter e garantir a manutenção contínua dos equipamentos (geradores, *nobreaks*, etc.) que alimentam a energia dos equipamentos computacionais dos locais destinados ao armazenamento das cópias de segurança do Poder Judiciário do Estado do Ceará; e

f) manter e garantir, nos locais destinados ao armazenamento das cópias de segurança do Poder Judiciário do Estado do Ceará, toda a infraestrutura predial necessária à segurança física e à proteção contra incêndios ou desastres/catástrofes naturais;

IV - da Gerência de Infraestrutura de Tecnologia da Informação:

a) homologar *software* para *backup*;

b) manter o registro de *softwares* homologados para *backup*;

c) realizar cópias de segurança (*backup*) das informações, *softwares*, imagens, áudio e vídeos, e testá-las regularmente, conforme plano de testes;

d) classificar e manter registro das cópias de segurança com atributos: permissão de acesso, data, tempo de retenção, local de armazenamento, prioridade de recuperação dos dados;

e) fornecer informações de *log* relativos a equipamentos e sistemas e redes computacionais do Poder Judiciário do Estado do Ceará no que diz respeito à execução de *software* de cópias de segurança;

f) assegurar-se de que a largura de banda da rede e o subsistema do disco sejam capazes de suportar uma quantidade grande de dados, tais como a recuperação do *backup* completo;

g) testar, mensalmente, em serviços críticos, de acordo com o Plano de Testes de Cópias de Segurança;

h) monitorar o ambiente de Tecnologia da Informação contra possíveis vulnerabilidades, invasões e ataques cibernéticos durante a execução dos *backups*;

i) garantir a execução de cópias de segurança e restauração das seguintes soluções tecnológicas:

1. sistemas judicias e administrativos (SJSA);

2. bases de dados dos sistemas judicias e administrativos (BDSJSA);

3. gravações telefônicas e outras ferramentas multicanais (*ominichannel*) das centrais de atendimento (GTFMCA);

4. todos os áudios e os vídeos relativos às audiências do processo eletrônico (AVPE);

5. áudios e vídeos de processos não eletrônicos, quando solicitado pelo(a) juiz(juíza) diretor(a) do Fórum ou juizado (AVNPE);

6. arquivos e pastas dos servidores de rede e sistemas de arquivos (APSA);

7. *e-mails* dos(as) usuários(as) e seus respectivos anexos que possuam conta no domínio tjce.jus.br (E-MAIL);

8. eventos (*logs*) das soluções de segurança, auditoria e acessos de toda as soluções mantidas pela Secretaria de Tecnologia da Informação e pela Gerência de Informática do Fórum Clóvis Beviláqua, de acordo com a legislação em vigor e as resoluções do Conselho Nacional de Justiça (LOGS); e

9. outras soluções autorizadas pelo(a) Secretário(a) de Tecnologia da Informação;

V - da Área de Segurança da Informação:

a) autorizar, após sua homologação, a utilização de *software* para *backup*;

b) definir quem faz a manipulação das mídias quando chegam às instalações de armazenamento;

c) fiscalizar o pessoal responsável pela guarda dos dados e exigir garantia de segurança junto à empresa que faz o transporte e o armazenamento;

d) prover os *softwares* e as mídias de *backup*; e

e) elaborar, testar e manter atualizado, conjuntamente com áreas da Secretaria de Administração e Infraestrutura e da Secretaria de Tecnologia da Informação, um plano de contingência para os locais destinados ao armazenamento das cópias de segurança do Poder Judiciário do Estado do Ceará que atenda no mínimo às seguintes situações: desastres/catástrofes naturais, atentados, incêndios, vandalismos, falta de energia ou problemas prediais e infraestruturais;

VI - do Comitê de Governança de Segurança da Informação e de Crises Cibernéticas: o comitê será acionado quando a área de Segurança da Informação julgar pertinente;

VII - do Monitoramento e da Auditoria do Ambiente: a auditoria será promovida pela área de Segurança da Informação, verificando a adoção das regras contidas no presente documento.

Art. 6° Penalidades: as penalidades poderão incluir processos administrativos, além de outras, cíveis ou criminais, previstas em lei.