RESOLUÇÃO Nº 39, DE 12 DE DEZEMBRO DE 2024.

Dispõe sobre a Política de Backup e Restauração de dados digitais do TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ – PSI/TCE-PI.

O TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ, no uso das atribuições legais e constitucionais; e,

Considerando que a informação gerada internamente, adquirida ou absorvida pelo Tribunal de Contas do Estado do Piauí, é patrimônio da Instituição e, portanto, necessita ser protegida;

Considerando que o Tribunal mantém grande volume de informações essenciais ao exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem manter-se íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

Considerando que as informações são armazenadas em diferentes suportes e veiculadas por diversas formas, tais como meio impresso, eletrônico e magnético, sendo, portanto, vulneráveis a desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

Considerando, por fim, que a ABNT NBR ISO/IEC 27002:2022, norma que estabelece boas práticas em segurança da informação, recomenda a definição de uma política backup e restauração de dados digitais;

RESOLVE:

Art. 1º Instituir a Política de Backup e Restauração de Dados Digitais (PBRDD- TCE/PI), objetivando assegurar que os softwares e sistemas, possuídos ou custodiados, serão protegidos e de forma a garantir sua recuperação em caso de perdas.

Art. 2º Esta política tem como objetivo divulgar toda a estratégia, incluindo diretrizes, responsabilidades e competências, para a realização de cópia de segurança (backup) de dados sensíveis ao negócio no ambiente corporativo do TCE-PI.

Art. 3º Para efeito desta Resolução, entende-se por:

I- **BACKUP OU CÓPIA DE SEGURANÇA:** Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação, assegurando a fidelidade do dado original. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

II- **BACKUP COMPLETO:** modalidade de backup em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup.

III- **BACKUP INCREMENTAL:** modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup de qualquer modalidade efetuado.

IV- **ROTINA DE BACKUP**: procedimento utilizado para se realizar um backup.

V- **RESTAURAÇÃO:** processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup**.**

VI- **RETENÇÃO:** período pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

VII- **CUSTODIANTE DA INFORMAÇÃO:** Qualquer indivíduo ou estrutura do

TCE-PI que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controle de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação.

VIII- **ELIMINAÇÃO:** Exclusão de dado ou conjunto de dados armazenados, independentemente do procedimento empregado. No contexto do TCE-PI, refere-se à destruição de dados que não são mais necessários para as atividades institucionais.

IX- **MÍDIA:** Mecanismos em que dados podem ser armazenados. Isso inclui discos rígidos, fitas magnéticas, CDs, DVDs e serviços de nuvem.

X- **INFRAESTRUTURA CRÍTICA**: Instalações, serviços, bens e sistemas, virtuais ou físicos, cuja incapacidade, destruição ou desempenho extremamente degradado podem causar sérios impacto social, econômico, político, internacional ou à segurança, especialmente nas atividades de fiscalização e controle do Tribunal.

XI- **RECOVERY POINT OBJECTIVE (RPO):** Ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente.

XII- **RECOVERY TIME OBJECTIVE (RTO):** Tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados após um incidente.

XIII- **BACKUPS DE ARQUIVAMENTO:** Estratégia de armazenamento de dados que se concentra na preservação e na retenção de informações para longos períodos, frequentemente para atender a requisitos legais, regulatórios ou de conformidade.

Art. 4º As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Art. 5º Os serviços de TI críticos do TCE-PI serão formalmente identificados pelo Comitê de Gestão de Tecnologia da Informação do Tribunal (CGTI), que é responsável por avaliar e classificar os sistemas e dados que necessitam de salvaguardas específicas.

Art. 6º Já ficam previamente estabelecidos como críticas as seguintes soluções e suas bases de dados: e-TCE, eProcesso, Site Institucional, Servidor de Arquivos e base de usuários (Active Directory).

Art. 7º Os fornecedores e desenvolvedores de sistemas devem documentar as melhores práticas de backup para seus respectivos sistemas.

Art. 8º As rotinas de backup devem utilizar soluções apropriadas e especializadas, preferencialmente de forma automatizada, para aumentar a eficiência e a confiabilidade do processo.

Art. 9º Compete à STI solicitar à Presidência do TCE-PI, com as justificativas pertinentes, os equipamentos e softwares necessários para manter o parque de ativos computacionais sempre atualizado e em quantidade necessária ao atendimento da demanda de backup.

Art. 10 Esta política se aplica a todos os servidores, colaboradores e

prestadores de serviços que têm acesso aos dados digitais do TCE-PI, incluindo aqueles que criam, processam ou armazenam dados de propriedade do Tribunal.

Art. 11 Dados armazenados localmente em microcomputadores de usuários ou em quaisquer outros dispositivos fora do Datacenter do TCE-PI não serão salvaguardados nem recuperados. A responsabilidade pela segurança e integridade desses dados recai sobre o indivíduo que utiliza tais dispositivos.

Art. 12 Os serviços de armazenamento de dados e/ou backup fornecidos pelo TCE-PI são para uso exclusivo de dados corporativos, sendo passíveis de auditoria.

Art. 13 Dados pessoais poderão ser excluídos sem aviso prévio e não poderão ser recuperados.

Art. 14 A salvaguarda de dados digitais que pertencem a serviços de TI do TCE-PI, mas que são custodiados por outras entidades, públicas ou privadas, como em casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre as partes envolvidas.

Art. 15 A Política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação do TCE-PI, garantindo que os dados sejam geridos de acordo com as diretrizes de segurança estabelecidas.

Art. 16 A Política deve estar integrada à gestão de continuidade de negócios do Tribunal, assegurando que a recuperação de dados não comprometa a continuidade das operações essenciais.

Art. 17 As rotinas de backup devem ter requisitos mínimos diferenciados com base na criticidade do tipo de serviço de TI ou dado a ser salvaguardado, dando prioridade aos serviços críticos do TCE-PI.

Art. 18 O armazenamento de backups deve ser realizado, sempre que possível, em um local distinto da infraestrutura crítica do Tribunal. É desejável que haja um site de backup em um local remoto para armazenar cópias extras dos principais backups, especialmente dos dados de serviços críticos.

Art. 19 A infraestrutura de rede utilizada para backup deve ser logicamente e fisicamente separada dos sistemas críticos do Tribunal, minimizando o risco de comprometimento dos dados.

Art. 20 Em situações em que a confidencialidade dos dados é crucial, cópias de segurança devem ser protegidas através de criptografia, garantindo que apenas usuários autorizados possam acessar as informações sensíveis.

Art. 21 A segurança dos dados de backup deve seguir práticas rígidas de controle de acesso, garantindo que apenas administradores autorizados tenham permissão para manipulá-los. É recomendável o uso do Princípio de Menor Privilégio (Principle of Least Privilege - PoLP), onde cada usuário possui apenas as permissões mínimas necessárias para executar suas funções.

Art. 22 Os backups dos serviços de TI críticos do Tribunal de Contas do Estado do Piauí devem ser realizados utilizando-se as seguintes frequências

temporais:

I - Horária;
II- Diária;
III-Semanal;
IV-Mensal;
V-Anual.

Art. 23 Os serviços de TI críticos da Tribunal de Contas do Estado do Piauí devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I- Diária: 7 dias;
II- Semanal: 30 dias;
III-Mensal: 7 dias;
IV-Mensal de arquivamento: 1 ano.
V-Anual de arquivamento: 5 anos.

Art. 24 Os backups são armazenados fisicamente em um servidor dedicado na sala cofre do Tribunal.

Art. 25 Cópias de segurança adicionais são mantidas em fitas e serviços de nuvem para redundância e integridade.

Art. 26 Para assegurar a continuidade das operações, a tabela a seguir define os limites de RPO e RTO para os principais sistemas críticos do TCE-PI:

Sistema	RPO (Intervalo de perda de dados)	RTO (Tempo de recuperação)
Sistema e-TCE	24 horas	10 horas e 51 minutos
Sistema e-Processo	12 horas	24 horas e 16 minutos
Admissão Controle	12 horas	24 horas e 16 minutos
Cadastro de Avisos	12 horas	24 horas e 16 minutos
Sagres Controle	12 horas	24 horas e 16 minutos
AR Digital	12 horas	24 horas e 16 minutos
Cadastro de UG	12 horas	24 horas e 16 minutos
Controle de Multas	12 horas	24 horas e 16 minutos
Diário Oficial - Administração	12 horas	24 horas e 16 minutos
Documentação Controle	12 horas	24 horas e 16 minutos
Emissão de Certidões	12 horas	24 horas e 16 minutos
Homologação de UGS e Usuários	12 horas	24 horas e 16 minutos
Impedimento	12 horas	24 horas e 16 minutos
Sagres Controle	12 horas	24 horas e 16 minutos
Cadastro Web	12 horas	24 horas e 16 minutos
Banco de Dados	12 horas	54 horas e 34 minutos
Egesp	1 semana	0:48:82 minutos
Arquivos de Configuração	1 semana	30 minutos
Pastas da rede	12 horas	19 horas e 47 minutos
Código fonte dos sistemas	12 horas	1 hora e 28 minutos
Outros sistemas	12 horas	24 horas e 16 minutos

Art. 27 Fica estabelecido como plano de backup vigente o que está definido na tabela a seguir:

Descrição	Frequência	Armazenamento	Retenção

Servidores de arquivos críticos	Diária	Disco	7 dias
Arquivos do eTCE	Diária	Disco + Nuvem	30 dias
Códigos-fonte das aplicações	Diária	Disco + Nuvem	30 dias
Arquivos do SEI	3 em 3 horas	Disco + Nuvem	30 dias
Servidor de Banco de Dados	12 em 12 horas	Disco	30 dias
Sistema eTCE	Primeiro domingo de cada mês	Disco	7 dias
Repositório de arquivos eTCEviewer	Primeiro sábado de cada mês	Disco	7 dias
Backup de todo o ambiente para arquivamento	Primeira segunda feira de cada mês / Anualmente no primeiro domingo de cada ano	Disco + Fita	12 Meses para backup mensais e 5 anos para backups anuais
Arquivos de configuração dos sistemas	Todos os sábados	Disco + Nuvem	28 dias
Backup de todo o ambiente para recuperação rápida	Todos os sábados	Disco	30 dias

Art. 28 Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 29 Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Art. 30 Deve-se manter uma reserva de recursos (físicos e lógicos) para a realização de testes de restauração de backup, assegurando que esses testes sejam realizados regularmente e sem impactar as operações.

Art. 31 Testes regulares são realizados a cada seis meses para verificar a eficácia dos processos de restauração.

Art. 32 Logs de backup são revisados diariamente para identificar problemas ou melhorias.

Art. 33 A equipe da Divisão de Redes e Segurança(DIRES) garantirá que a mídia a ser descartada não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

Art. 34 A DIRES garantirá a destruição física da mídia antes do descarte.

Art. 35 O descarte da mídia deve seguir as diretrizes estabelecidas pelo Tribunal de Contas do Estado do Piauí, incluindo a documentação do processo de descarte e a verificação da destruição efetiva, para assegurar a conformidade com

as normas de segurança da informação e proteção de dados.

Art. 36 O administrador de backup e o operador de backup devem ser capacitados nas tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Art. 37 O administrador e o operador de backup do TCE-PI serão indicados pelo CGTI e nomeados pelo Presidente, entre os servidores de carreira lotados na STI.

Art. 38 Caso não seja possível a indicação de empregados distintos, o mesmo empregado poderá exercer os papéis de administrador e operador de backup desde que não conflite com outras funções do funcionário.

Art. 39 São atribuições do Administrador de Backup:
I- Propor soluções de cópia de segurança das informações digitais produzidas ou custodiadas pelo Tribunal de Contas do Estado do Piauí;
II-Providenciar a criação e manutenção dos backups;
III-Configurar as soluções de backup;
IV-Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
V-Definir os procedimentos de restauração e auxiliar nos mesmos.
VI-Propor modificações visando ao aperfeiçoamento desta Política de Backup e Recuperação de Dados Digitais;

Art. 40 São atribuições do operador de backup:
I- Restaurar ou recuperar os backups em caso de necessidade;
II-Operar e manusear as unidades de armazenamento de backups;
III-Verificar diariamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;
IV-Gerenciar mensagens e registros de auditoria (logs) diários dos backups;
V-Informar ao administrador de backup qualquer problema que impossibilite a restauração de um backup.

Art. 41 A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 42 A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de backup. A aprovação para execução da alteração depende da anuência do gestor da informação e de prévia apreciação pelo CGTI.

Art. 43 O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do TCE-PI, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da organização.

Art. 44 A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

Art. 45 O período de janela de backup deve ser determinado pelo

administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados do TCE- PI.

Art. 46 O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 47 Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos gestores das informações.

Art. 48 As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, uso de criptografia e com acesso restrito a pessoas autorizadas pelo administrador de backup.

Art. 49 Esta Política deverá ser revisada anualmente. Contudo, quando identificada a necessidade de alteração em qualquer de seus dispositivos, poderá ser atualizada a qualquer tempo.

Art. 50 Casos excepcionais não abordados neste documento serão decididos pelo CGTI, com análise da Secretaria de Tecnologia da Informação, e sendo necessário, pelas demais Divisões de TI ou pelos gestores das informações digitais.

Art. 51 Esta resolução entrará em vigor na data de sua publicação, ficando revogadas as disposições em contrário.

Sala das Sessões do Tribunal de Contas do Estado do Piauí, em Teresina, 12 de dezembro de 2024.

Consª. Waltânia Maria Nogueira de Sousa Leal Alvarenga - **Presidente em exercício**
Cons. Abelardo Pio Vilanova e Silva
Consª. Lilian de Almeida Veloso Nunes Martins
Consª. Rejane Ribeiro Sousa Dias
Cons. Substituto Jaylson Fabianh Lopes Campelo
Cons. Substituto Jackson Nobre Veras
Cons. Substituto Alisson Felipe de Araújo
Proc. Plínio Valente Ramos Neto – **Procurador-Geral do MPC**

Este texto não substitui o publicado no DO TCE/PI de 16.12.24.