

**RESOLVE:**

~~Art. 1º Instituir, no âmbito deste Tribunal, Comissão de Gestão do Teletrabalho (CGT) com a finalidade de assegurar a utilização adequada do teletrabalho, observadas as atribuições constantes na Portaria nº 930/2023.~~

~~Art 2º Designar os(as) seguintes membros(as) para a comissão:~~

~~I— Glória Cristina Santana Tourinho, titular da Secretaria de Gestão de Pessoas;~~

~~II— Thalita Fernandes Tosta Maciel, na qualidade de representante da Presidência;~~

~~III— Maria do Socorro Carvalho Cruz Medeiros de Almeida Gouveia, na qualidade de representante da Corregedoria Regional Eleitoral;~~

~~IV— Ronildo de Queiroz Dantas, na qualidade de representante da Diretoria-Geral;~~

~~V— André Luiz Cavalcanti e Cavalcante, na qualidade de representante da Secretaria de Tecnologia da Informação e Comunicação.~~

~~Parágrafo único. A coordenação da comissão ficará sob a responsabilidade da servidora Glória Cristina Santana Tourinho, titular da Secretaria de Gestão de Pessoas, que, em seus afastamentos, será substituída por seu (sua) substituta(o) legal.~~

~~Art. 3º Esta portaria entra em vigor na data de sua publicação.~~

~~Salvador, 17 de novembro de 2023~~

~~Des. ROBERTO MAYNARD FRANK~~

~~Presidente do Tribunal Regional Eleitoral da Bahia~~

**PORTARIA TRE-BA Nº 957, DE 16 DE NOVEMBRO DE 2023**

~~Altera a Portaria n.º 356, de 04 de julho de 2018, que institui Normas de Segurança da Informação (NSI) no âmbito do Tribunal Regional Eleitoral da Bahia, para inclusão do Anexo XIV.~~

~~O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DA BAHIA, no uso das atribuições regimentais,~~

~~CONSIDERANDO o disposto na Resolução TSE n.º 23.644, de 1º de julho de 2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;~~

~~CONSIDERANDO o disposto na Portaria n.º 405, de 17 de agosto de 2021, que regulamenta a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral da Bahia; e~~

~~CONSIDERANDO o disposto no Processo SEI n.º [0010636 34.2023.6.05.8000](#),~~

**RESOLVE**

~~Art. 1º Alterar a Portaria n.º 356, de 04 de julho de 2018, da Presidência, para inclusão do Anexo XIV (NSI-014 — Armazenamento em Serviços de Computação em Nuvem), com redação constante no apêndice deste normativo.~~

~~Art. 2º Esta Portaria entrará em vigor na data de sua publicação.~~

~~Salvador, em 16 de novembro de 2023.~~

~~Des. ROBERTO MAYNARD FRANK~~

~~Presidente do Tribunal Regional Eleitoral da Bahia~~

**ANEXO XIV****NSI-014 - ARMAZENAMENTO EM SERVIÇOS DE COMPUTAÇÃO EM NUVEM****1. OBJETIVO**

Esta norma estabelece diretrizes de segurança da informação para o armazenamento de dados em serviços de computação em nuvem, quando o uso de contas pessoais é cedido, com ênfase na proteção de dados pessoais (DP) de servidores, juízes, colaboradores terceirizados e estagiários.

**2. ÂMBITO**

Esta norma se aplica a todas as unidades e colaboradores da organização responsáveis pelo armazenamento de dados em serviços de computação em nuvem.

**3. CONCEITOS E DEFINIÇÕES**

3.1. Computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN).

3.2. Operador de DP: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

3.3. Provedor de serviços de nuvem: ente, público ou privado, que fornece uma plataforma, infraestrutura, aplicativo, serviços de armazenamento ou ambientes de tecnologia da informação baseados em nuvem.

3.4. A computação em nuvem é composta pelos seguintes modelos de implantação:

3.4.1. Nuvem Comunitária: infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos;

3.4.2. Nuvem Híbrida: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;

3.4.3. Nuvem Privada (ou interna): infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

3.4.4. Nuvem Pública (ou externa): infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas;

#### 4. DIRETRIZES DE SEGURANÇA

4.1. Características essenciais de computação em nuvem:

4.1.1. Autosserviço sob demanda - O cliente pode pessoalmente configurar recursos computacionais necessários, como servidores e redes de armazenamento, de maneira automática, sem precisar depender do fornecedor de serviços em nuvem.

4.1.2. Amplo acesso pela internet - Os recursos computacionais estarão disponíveis através da internet, podendo ser livremente acessados por diferentes dispositivos, independente de seu fabricante.

4.1.3. Rápida Elasticidade - As capacidades dos recursos poder ser facilmente aumentadas ou diminuídas de acordo com a demanda e perfil de uso das aplicações. Essas alterações podem ser realizadas a qualquer momento, possibilitando melhor utilização e, portanto, menor custo.

4.1.4. Serviço mensurado - Os sistemas em nuvem controlam e aperfeiçoam a utilização de recursos automaticamente, considerando capacidades de monitoramento apropriado para cada serviço. O uso dos recursos pode ser auditado, permitindo transparência para o fornecedor e para o cliente.

4.1.5. Pool de recursos - Os recursos do fornecedor de serviços em nuvem são disponibilizados para servir a diferentes categorias de clientes usando um modelo exclusivo (*single-tenant*) ou compartilhado (*multi-tenant*), conforme necessidade, sejam recursos físicos ou virtuais.

4.2. Contas de Computação em Nuvem

4.2.1. É estritamente proibido o uso de contas pessoais para armazenar dados institucionais ou dados pessoais de servidores, juízes, colaboradores terceirizados e estagiários.

4.2.1.1. O incidente de segurança da informação no Tribunal resultante da violação ao disposto no item 4.2.1 sujeitará o usuário responsável às penalidades cabíveis.

4.2.2. A organização fornecerá contas de computação em nuvem dedicadas e devidamente configuradas aos colaboradores autorizados, de acordo com suas funções e níveis de acesso.

4.2.3. As contas de computação em nuvem fornecidas pela organização devem ser protegidas por senhas fortes, não devendo ser compartilhadas com terceiros.

#### 4.3. Classificação e Proteção de Dados

4.3.1. Todos os dados armazenados em serviços de computação em nuvem devem ser adequadamente classificados de acordo com a política de classificação de informações da organização.

4.3.2. Os dados pessoais de servidores, juízes, colaboradores terceirizados e estagiários devem ser tratados como informações sensíveis e devem receber proteção especial.

4.3.3. A criptografia de dados em trânsito e em repouso deve ser implementada para garantir a integridade e a confidencialidade das informações.

#### 4.3. Acesso e Controle de Dados

4.3.1. O acesso aos dados armazenados em serviços de computação em nuvem deve ser concedido somente a colaboradores autorizados, com base no princípio do acesso mínimo necessário.

4.3.2. Deve ser implementado um controle rigoroso de acesso, utilizando autenticação multifator sempre que possível.

4.3.3. As permissões de acesso devem ser revisadas periodicamente e ajustadas de acordo com as mudanças nas funções e responsabilidades dos colaboradores.

#### 4.4. Monitoramento e Auditoria

4.4.1. Deve ser implementado um sistema de monitoramento contínuo para detectar atividades suspeitas ou não autorizadas no armazenamento em nuvem.

4.4.2. Logs de atividades devem ser mantidos e revisados regularmente para identificar possíveis violações de segurança e garantir a conformidade com as políticas estabelecidas.

### 5. SEGURANÇA DA INFORMAÇÃO

5.1. Incidentes de Segurança da Informação devem ser imediatamente comunicados ao Comitê de Governança de Segurança da Informação (CGSI) para apuração e consequente adoção das providências cabíveis.

5.2. O provedor de nuvem deverá observar padrões de segurança, diretrizes e controles estabelecidos nas normas ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 e demais legislações correlatas.

5.3 Em se tratando de armazenamento de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.

5.4 Devem ser observados os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem previstos na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021.

### 6. RESPONSABILIDADES

6.1. Da Secretaria de Tecnologia da Informação e Comunicação (STI):

6.1.1. Gerenciar o acesso dos usuários ao serviço em nuvem.

6.1.2. Comunicar ao CGSI os incidentes cibernéticos informados pelo provedor de serviço de nuvem.

6.2. Do Operador de Dados Pessoais (DP) em nuvem.

6.2.1. É vedada a utilização de DP tratados em nuvem pública para fins de marketing e publicidade, sem consentimento expresso.

6.2.2. Informar à Ouvidoria, *Data Protection Officer - DPO* do TRE-BA, qualquer acesso não autorizado aos DP ou acesso não autorizado aos equipamentos ou instalações de tratamento que resulte em perda, divulgação ou alteração de DP.

## 7. VIGÊNCIA E ATUALIZAÇÃO

A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

# ATOS DO CORREGEDOR REGIONAL ELEITORAL

## EDITAIS

### **EDITAL TRE-BA Nº 101, DE 20 DE NOVEMBRO DE 2023**

~~PROGRAMAÇÃO DA AUDIÊNCIA PÚBLICA E DIVULGAÇÃO DE INSCRIÇÕES DEFERIDAS E ORDEM DE MANIFESTAÇÃO NA AUDIÊNCIA PÚBLICA~~

~~O VICE PRESIDENTE E CORREGEDOR REGIONAL ELEITORAL DA BAHIA, DES. ABELARDO PAULO DA MATTA NETO, no uso de suas atribuições legais e regimentais e em conformidade com o disposto no Edital nº 99/2023/TRE-BA,~~

~~TORNA PÚBLICO programação da Audiência Pública presidida pelo Corregedor Regional Eleitoral da Bahia, nos termos da Portaria nº 940/2023, e art. 5º, do Provimento nº 01/2022, da Corregedoria Geral da Justiça Eleitoral, na oportunidade em que pronunciar-se-ão as autoridades e as inscritas e os inscritos para manifestação de forma oral, que ocorrerá no dia 30 de novembro de 2023 na Câmara Municipal de Paulo Afonso, localizado na Avenida Apolônio Sales, nº 495 – Centro, com horário de início às 18h.~~

~~TORNA PÚBLICO, ainda, relação das inscrições deferidas e ordem de manifestação para uso da fala na Audiência Pública, a seguir:~~

	NOME
1	Leana Bezerra Gomes Evangelista
2	Albérico Oliveira Evangelista
3	Marcos Antonio Barbosa e Silva
4	Edilson Vieira
5	Alicia Reana dos Santos Martins
6	Sydney Correia Leão
7	Maurício Lins Aroucha
8	Pedro Gerônimo Estevão Pereira
9	Antônia Jane de Araujo Santos
10	Marcondes Teixeira Lima
11	Mivaldo Pereira da Silva
12	Thiago Santos da Silva
13	Maria Vicentina Santos Silva
14	Sara da Conceição Silva Gomes
15	Janisabel da Assunção Sousa Araújo de Carvalho
16	Elton Rocha Moraes da Silva
17	Milton Santos Nascimento
18	Pedro Vinícius dos Santos Silva