Sumário Executivo

TRIBUNAL DE JUSTIÇA DO ESTADO DE SERGIPE

Departamento de Auditoria Interna

# Gestão do Sistema de Informações e Proteção de Dados

Janeiro/2026

## 1 - Contextualização

- Processo SEI nº: 0020596-67.2025.8.25.8825
- Natureza: Auditoria Ordinária (PAA 2025)
- Objeto: Gestão do Sistema de Informações e Proteção de Dados
- Unidades Interessadas: CGPDP, SETECI e DIGEPE
- Período: 06/08/2025 a 26/01/2026

## 2 - Objeto da Auditoria

Avaliar, no âmbito do Tribunal de Justiça do Estado de Sergipe, a conformidade dos normativos de Segurança da Informação e Proteção de Dados com os dispositivos da Lei Geral de Proteção de Dados (Lei nº 13.709/18) - LGPD e a Resolução CNJ nº 363/2021.

## 3 - Destaques Positivos (Avanços)

Os trabalhos de avaliação mostraram avanços significativos na conformidade formal e estrutural:

- **Estrutura Administrativa Instituída:** Instâncias de governança estabelecidas e em pleno funcionamento, incluindo os comitês de Governança de TIC, Gestão de TIC, Crises Cibernéticas, Gestão de Riscos e o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais.

- **Base Normativa Consolidada**: Regulamentação estabelecida para tratar os temas de segurança e privacidade através de Resolução, Instrução Normativa, Portaria e Políticas (Política de Privacidade e Proteção de Dados Pessoais - PPPDP, Política de Segurança da Informação - PSI e Política de Segurança do Usuário - PSU).

- **Gestão via Sistema MentoRH:** Utilização de plataforma que permite a gestão do ciclo de vida dos dados pessoais, garantindo a centralização de dados, acessibilidade, transparência e a padronização de processos.

- **Segurança da Informação (Protocolos):** Implementação de criptografia em trânsito (uso do protocolo SSL) e existência de mecanismos de Controles de Acesso Lógico baseados no princípio do menor privilégio.

## 4 - Principais Constatações (Achados)

Os resultados de Conformidade e Operacionalização apontaram um vácuo operacional entre a base normativa e a execução técnica auditável, com evidências para:

**Eixo I: Governança, Conformidade Normativa e Gestão de Terceiros**

Desatualização de normativos (como a Resolução 16/2012 e a IN 9/2017), ausência de definição clara de competências dos Comitês Gestores, falta de um grupo técnico de apoio ao Encarregado(DPO) e de um programa contínuo de capacitação e conscientização sobre a LGPD para o corpo funcional e terceirizados. Além disso, o mapeamento de processos de trabalho está defasado e incompleto no tocante ao tratamento de dados pessoais.

**Eixo II: Resposta a Incidentes e Gerenciamento de Riscos**

Inexistência de uma Metodologia de Gestão de Riscos específica para Privacidade, falta de formalização do "Apetite e Tolerância a Risco" e ausência de Relatórios de Impacto à Proteção de Dados (RIPD) para operações críticas. Identificou-se a falta de um plano operacional detalhado para notificação de incidentes à ANPD e aos titulares.

**Eixo III: Atendimento, Fiscalização e Responsabilização**

Fragilidade nos canais de atendimento aos direitos dos titulares (integração Ouvidoria-DPO), insuficiência de mecanismos de monitoramento contínuo e ausência de fluxos disciplinares específicos para violações de dados pessoais. Há também uma lacuna procedimental para o atendimento tempestivo de diligências de órgãos externos (ANPD/Tribunais de Contas), bem como alta probabilidade de Riscos Reputacional e de Sanções e Responsabilidade Civil (Accountability).

**Eixo IV: Ciclo de Vida do Tratamento de Dados no Sistema MentoRH**

O sistema MentoRH apresenta desconformidades graves, incluindo: ausência de ROPA e de inventário de dados sensíveis; falta de mecanismos para descarte irreversível (exclusão física) ou anonimização de dados (Tabela de temporalidade); e ausência de criptografia de dados em repouso.

## 5 - Recomendações (Pontos Críticos)

**Eixo I: Governança, Conformidade Normativa e Gestão de Terceiros**

Estabelecer cronograma formal de revisão normativa; atualizar as atribuições dos Comitês e do DPO; instituir um Plano Anual de Capacitação e um Plano de Conscientização; e concluir o Registro de Operações de Tratamento de Dados (ROPA).

**Eixo II: Resposta a Incidentes e Gerenciamento de Riscos**

Instituir formalmente a Metodologia de Gestão de Riscos de Privacidade; elaborar a Declaração de Apetite a Riscos (RAS); formalizar o Plano de Resposta a Incidentes de Privacidade (PRIP) e protocolos de comunicação com a ANPD/titulares; e incluir a obrigatoriedade do RIPD nos fluxos de trabalho.

**Eixo III: Atendimento, Fiscalização e Responsabilização**

Padronizar formulários para exercício de direitos (Art. 18 LGPD); formalizar a Ouvidoria como porta de entrada oficial; instituir procedimentos de fiscalização contínua; e criar protocolos de cooperação externa com prazos rígidos para resposta.

**Eixo IV: Ciclo de Vida do Tratamento de Dados no Sistema MentoRH**

Implementar a Tabela de Temporalidade para expurgo de dados; adotar criptografia em repouso no banco de dados; instituir auditorias periódicas de acesso e integrar o cancelamento de perfis ao fluxo de desligamento de pessoal.

## 6 - Conclusão

A auditoria avaliou a Gestão do Sistema de Informações e Proteção de Dados no Tribunal de Justiça do Estado de Sergipe. (TJSE).

O diagnóstico geral apontou que, embora coexistam base normativa para tratar os temas de segurança e privacidade de dados e estrutura administrativa com instâncias de governança estabelecidas e em pleno funcionamento, existe um vácuo operacional entre a teoria (normas) e a prática (segurança efetiva) devido à falta de formalização de processos operacionais e monitoramento técnico contínuo.

Nesse diapasão, a transição da "conformidade documental" para a "conformidade efetiva" e auditável reveste-se, portanto, como o principal desafio a ser administrado pela Alta Administração, Comitês de Segurança da Informação e Gestor de Privacidade e Proteção de Dados Pessoais e áreas técnicas (Seteci e Digepe).