



GABINETE DAVICE-PRESIDÊNCIA
CENTRO DE INTELIGÊNCIA DA JUSTIÇA ESTADUAL DO CEARÁ (CIJECE)

NOTA TÉCNICA Nº 11/2025.

Assunto: Protocolos de Segurança Cibernética no âmbito do Processo Judicial Eletrônico do TJCE (PJe e SAJ).

Ementa: ESTABELECIMENTO DE DIRETRIZES E PROTOCOLOS DE SEGURANÇA CIBERNÉTICA PARA O PROCESSO JUDICIAL ELETRÔNICO DO TJCE (PJe E SAJ). ANÁLISE DE RISCOS, MEDIDAS DE PROTEÇÃO E RECOMENDAÇÕES PARA GARANTIR A INTEGRIDADE, CONFIDENCIALIDADE E DISPONIBILIDADE DOS DADOS JUDICIAIS.

Relator: FABRÍCIO VASCONCELOS MAZZA.

Revisor: ROBERTA PONTE MARQUES MAIA.

1. INTRODUÇÃO

A crescente digitalização dos processos judiciais, com a implementação do PJe e SAJ no TJCE, exige a adoção de medidas robustas de segurança cibernética para proteger os dados sensíveis e garantir a continuidade dos serviços. Esta nota técnica tem como objetivo estabelecer diretrizes e protocolos de segurança cibernética para o PJe e SAJ, visando mitigar riscos e assegurar a integridade, confidencialidade e disponibilidade dos dados judiciais.

2. PROTOCOLOS DE SEGURANÇA CIBERNÉTICA

Os protocolos de segurança cibernética para o PJe e SAJ devem abranger os seguintes aspectos:

- **Autenticação e Controle de Acesso:**

- ⑩ Implementação de autenticação multifator para acesso aos sistemas (preferência para Token instalado em celular).
- ⑩ Definição de perfis de acesso com base em funções e responsabilidades, sem prejuízo de acessibilidade ampla para Magistrados.
- ⑩ Revisão periódica dos perfis de acesso e revogação de acessos desnecessários, notadamente para estagiários.

- **Proteção de Dados:**

- ⑩ Criptografia de dados em repouso e em trânsito.
- ⑩ Implementação de políticas de backup e recuperação de dados.
- ⑩ Anonimização ou pseudonimização de dados sensíveis, quando necessário.

- **Deteccção e Resposta a Incidentes:**

- ⑩ Monitoramento contínuo dos sistemas para deteccção de atividades suspeitas.
- ⑩ Implementação de um plano de resposta a incidentes cibernéticos.
- ⑩ Realização de testes de intrusão e simulações de ataques cibernéticos.

- **Segurança de Rede:**

- ⑩ Implementação de firewalls e sistemas de deteccção de intrusão.
- ⑩ Segmentação da rede para isolar sistemas críticos.
- ⑩ Atualização regular de softwares e firmwares.

- **Conscientização e Treinamento:**

- ⑩ Treinamento contínuo dos servidores e usuários sobre segurança cibernética.
- ⑩ Divulgação de boas práticas de segurança cibernética.
- ⑩ Realização de campanhas de conscientização sobre phishing e outros ataques.

- **Conformidade com a LGPD e outras regulamentações:**

- ⑩ Adequação dos sistemas e processos às exigências da Lei Geral de Proteção de Dados (LGPD).
- ⑩ Acompanhamento das atualizações e novas regulamentações sobre segurança cibernética.

3. RECOMENDAÇÕES

Para a implementação eficaz dos protocolos de segurança cibernética, recomenda-se:

- ⑩ Realização de auditorias de segurança cibernética periódicas.
- ⑩ Investimento em tecnologias de segurança cibernética de última geração.
- ⑩ Criação de políticas internas de segurança cibernética, e seu constante aperfeiçoamento.

4. CONCLUSÃO

A segurança cibernética é fundamental para garantir a confiança e a integridade do processo judicial eletrônico. A implementação de protocolos robustos e a adoção de medidas preventivas são essenciais para proteger os dados judiciais e assegurar a continuidade dos serviços.

Fortaleza, 10 de Março de 2025.

**Centro de Inteligência do Tribunal de Justiça do Estado do
Ceará**

Grupo Decisório



GABINETE DAVICE-PRESIDÊNCIA
CENTRO DE INTELIGÊNCIA DA JUSTIÇA ESTADUAL DO CEARÁ (CIJECE)

Desembargador Francisco Mauro Ferreira Liberato
Vice-Presidente

Desembargador Fernando Luiz Ximenes Rocha
Presidente da Seção de Direito Público

Desembargador Emanuel Leite Albuquerque
Presidente da Seção de Direito Privado

Desembargador Mario Parente Teófilo Neto
Presidente da Seção de Direito Criminal

Grupo Operacional

Fabício Vasconcelos Mazza
Juiz de Direito

Roberta Ponte Marques Maia
Juíza de Direito