



## SUMÁRIO EXECUTIVO – Auditoria Secin n. 1/2025

### Processo eDoc n.

218032/2026

### O que a Secin recomenda

Auditoria sobre o processo "Gerir Incidentes e Requisições de Serviços de TIC".

### Por que esta auditoria foi realizada?

O processo auditado apresenta elevada materialidade financeira, operacional e institucional. Além de envolver contratos com valor anual da ordem de R\$ 13 milhões, o processo sustenta atividades críticas da Câmara dos Deputados, impactando diretamente, por exemplo, a realização de sessões de Plenário e reuniões de comissões. Ademais, é essencial para a operação segura de aproximadamente 12 mil estações de trabalho, com uma média superior a 3,7 mil atendimentos mensais a usuários dos serviços de TIC. Eventuais fragilidades em sua execução podem resultar em prejuízos financeiros, riscos à segurança da informação e comprometimento da continuidade de serviços institucionais críticos, com potencial reflexo negativo sobre a integridade institucional.

### O que a auditoria constatou?

O processo suporta de maneira eficaz a operação cotidiana, contribuindo para a continuidade das funções críticas da Câmara dos Deputados. Porém, foram detectadas as seguintes fragilidades, que demandam aperfeiçoamento para a adequada mitigação dos riscos residuais:

- 1) Deficiências nos procedimentos de registro, classificação, priorização e documentação de chamados, impactando a eficiência do processo.
- 2) A ferramenta de gerenciamento de incidentes e requisições (OTRS) encontra-se em versão obsoleta e sem suporte do desenvolvedor.
- 3) Os procedimentos de acesso remoto para atendimento de incidentes não possuem mecanismo de gravação de sessões, nem registro das ações realizadas.
- 4) Deficiência no registro do controle de verificação dos indicadores de qualidade apresentados pela contratada (fiscalização técnica).

### À Ditec:

- Elaborar e publicar a norma complementar prevista no art. 8º da Instrução Cenin n. 1, de 21/05/2012, tratando, no mínimo, sobre os seguintes temas relativos ao processo:
  - definição de papéis e responsabilidades;
  - procedimentos operacionais padronizados de documentação dos chamados;
  - critérios objetivos de classificação e priorização;
  - fluxos e prazos para escalonamento;
  - regras para gestão e utilização da base de conhecimento;
  - exigência de manuais técnicos para soluções atendidas;
  - padrões de comunicação com usuários do serviço;
  - critérios e requisitos para encerramento de chamados;
  - monitoramento e controle, com indicadores aferidos de maneira fidedigna e eventuais ações corretivas;
  - programa de capacitação contínua de atendentes;
  - periodicidade de revisão da norma e procedimentos.
- Realizar a atualização da ferramenta OTRS para versão suportada pelo fornecedor ou a migração para solução equivalente, assegurando a disponibilidade de suporte técnico e atualizações regulares de segurança.
- Estabelecer política de gestão de ciclo de vida de software crítico.
- Implementar política de gestão segura de acesso privilegiado remoto, prevendo:
  - Controle de acesso e autenticação;
  - Rastreabilidade;
  - Monitoramento;
  - Conscientização e responsabilização.
- Estabelecer diretrizes, modelos de formulários e relatórios de avaliação de qualidade dos serviços.
- Registrar no repositório institucional e no eDoc a atividade de controle de revisão dos indicadores de qualidade apresentados pela contratada.