



Auditoria sobre a gestão e governança do processo de trabalho “desenvolver e implementar níveis e estratégias de proteção de dados, segurança e privacidade”.

POR QUE ESTA AUDITORIA FOI REALIZADA

O objetivo principal desta ação foi avaliar os controles internos vinculados aos aspectos de governança e de gestão do processo de trabalho de desenvolver e implementar níveis e estratégias de proteção de dados, segurança e privacidade.

O QUE A AUDITORIA CONSTATOU

- 1) ausência de diretrizes básicas de construção de soluções de TIC para a Casa;
- 2) as responsabilidades para execução das ações de segurança da informação não estão bem definidas; e
- 3) lacuna na realização de reuniões ordinárias realizadas pelo CGSI.

BOAS PRÁTICAS

No decorrer da auditoria, foram identificadas boas práticas de gestão, que efetivamente contribuem para a mitigação de alguns riscos:

- a. reuniões do Comitê Gestor de Segurança da Informação (CGSI) e do Comitê de Gestão Estratégica (CGE) demonstrando a importância da governança e da gestão da segurança da informação percebida pela alta administração da Casa;
- b. normatização dos procedimentos e regras para fins de prevenção à infecção e à propagação do covid-19 no âmbito da Câmara dos Deputados, com emprego de teletrabalho; e
- c. normatização das atribuições e responsabilidades sobre soluções de Tecnologia da Informação e Comunicação (TIC).

O QUE A SECIN RECOMENDA

À DG:

- Elaborar normativo estabelecendo as diretrizes mínimas para as soluções desenvolvidas por unidades de TIC descentralizadas, permitindo melhor controle das políticas, regras e padrões institucionais relativos, entre outros temas, à segurança da informação. Prazo para implementação da recomendação: 180 dias.
- Identificar a(s) unidade(s) organizacional(is) responsável(is) pela implementação das ações de segurança da informação em nível corporativo, com as respectivas competências, como é o caso das ações preconizadas pelo PASI. Prazo para implementação da recomendação: 180 dias.
- Avaliar o disposto na Portaria n. 407, de 30/9/2013, no tocante às reuniões do CGSI. Prazo para implementação da recomendação: 90 dias.

Ao CGSI:

- Revisar e atualizar o Plano de Ação em Segurança da Informação (PASI), refletindo as atuais demandas institucionais. Prazo para implementação da recomendação: 180 dias.
- Observar o calendário de reuniões previsto em sua portaria de instalação e funcionamento. Prazo para implementação da recomendação: 90 dias.