TCU publica relatório avaliando as práticas de segurança cibernética da administração pública federal e reconhece situação “preocupante”

14.09.2022 2 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Informativos Proteção de Dados e Cybersecurity

No dia 16 de agosto, o Tribunal de Contas da União (TCU) publicou um documento intitulado "Cinco Controles de Segurança Cibernética para Ontem". Trata-se de uma análise do TCU acerca do nível de proteção cibernética da administração pública federal, apontando também medidas que devem ser tomadas o mais rápido possível.

O TCU promoveu sua fiscalização com base em 5 controles de segurança cibernética críticos, de um total de 18, recomendados pelo *Center for Internet Security*, organização estadunidense sem fins lucrativos que atua na promoção da cibersegurança e cujas recomendações são tidas como "pontos de partida" básicos para um ecossistema seguro, a fim de identificar o grau de proteção de 377 organizações públicas federais. Neste primeiro ciclo, o TCU avaliou dos seguintes controles críticos:

- **Inventário e controle de ativos corporativos.** Organizações devem gerenciar os equipamentos conectados à sua rede, como computadores, dispositivos de conexão e servidores. Medidas simples, como manter um inventário dos dispositivos conectados ao sistema e excluir os não autorizados, foram indicadas.
- **Inventário e controle de ativos de software.** Organizações devem gerenciar os sistemas operacionais e aplicativos utilizados. O TCU aponta que softwares desatualizados podem ser explorados por hackers. Um navegador web com vulnerabilidades, por exemplo, pode ser a porta de entrada para um ataque de phishing.
- **Gestão contínua de vulnerabilidades.** Organizações devem gerenciar ativamente a atualização de dispositivos e softwares a fim de identificar vulnerabilidades. O TCU indica, dentre outros, a execução de uma gestão automatizada de correção (patches) dos programas e softwares.
- **Conscientização sobre segurança e treinamento de competências.** Organizações devem manter um programa contínuo para que os colaboradores tenham condutas adequadas à segurança da informação e cibernética. Como medidas básicas, apontam-se treinamentos sobre o tratamento de dados, o reconhecimento de incidentes, etc.
- **Gestão de respostas a incidentes.** Organizações devem ser capazes de identificar potenciais ameaças, evitando que se espalhem e recuperando rapidamente eventuais dados e sistemas corrompidos, sendo essencial manter um plano de resposta a incidentes.

Ao fim, o TCU concluiu que 24% das organizações públicas federais

analisadas possuem um grau de proteção cibernética "inexpressivo", seguidas por 54% que ainda possuem um grau "inicial" de cibersegurança. Com apenas 4% de organizações atingindo o nível "aprimorado" de segurança cibernética, o TCU afirma que a situação é "preocupante". De todo modo, análises futuras ainda devem ser feitas com base nos outros controles críticos.

- **Para ler o documento do TCU, clique aqui.**

Este conteúdo faz parte do Informativo de Proteção de Dados. Clique aqui para ler mais notícias.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares