Auditoria à segurança dos sistemas de informação do Instituto de Financiamento da Agricultura e Pescas, IP (IFAP)

SÍNTESE DE RESULTADOS

Esta ação teve como objetivos analisar a segurança dos sistemas de informação e a conformidade dos mesmos face ao padrão internacional ISO/IEC 27001:2013. Esta ação incidiu sobre o exercício financeiro de 2015.

1. Principais conclusões

A maturidade da segurança dos sistemas de informação do IFAP, com base no modelo "Capability Maturity Model" – corresponde ao nível "(3) – procedimento integrado", considerando a existência de normas e a implementação dos respetivos procedimentos. Não foram aprovadas formalmente as políticas e normas baseadas na ISO/IEC 27001:2013, elaboradas pelos responsáveis pela segurança da informação. Não foi realizado um simulacro para testar, ajustar e alinhar o Plano de Continuidade do Negócio com as necessidades operacionais do IFAP. O IFAP dispõe de um Plano de Continuidade do Negócio (processo continuo) mas, falta integrá-lo num conjunto mais alargado de medidas do controlo de gestão. O IFAP não implementou nem testou planos parcelares para:

a. Dispor de procedimentos de emergência com a descrição das equipas que os executam.

b. Implementar operações de recuperação e regresso à normalidade.

c. Realizar operações de deteção de vulnerabilidades técnicas, de forma a minimizar o risco de incidentes de segurança, em particular, nas aplicações que processem ou tenham impacto em ativos organizacionais críticos para o negócio.

2. Principais recomendações à/s entidade/s auditada/s

A aprovação formal das políticas baseadas na ISO/IEC 27001:2013. A Implementação do Plano de Continuidade do Negócio, em conjunto com medidas do controlo de gestão que permitam a deteção de ameaças e respetiva mitigação de riscos, de modo a controlar os custos orçamentais e a aplicação das boas práticas na gestão do negócio. A realização do simulacro do Plano de Continuidade do Negócio, o qual deve englobar: Estratégias de proteção – Contingência, recuperação e regresso à normalidade; Gestão de Crise; Atualização do Plano. A criação e teste de um conjunto de planos parcelares. A atualização do plano global de segurança.

(Relatório n.º 565/2016, homologado, por S. Ex.ª Secretário de Estado do Orçamento, em 2016-09-08).