Segurança dos sistemas de informação do IFAP

SÍNTESE DE RESULTADOS

Auditoria aos sistemas de informação utilizados pelo IFAP na gestão do FEAGA e do FEADER, tendo por base os requisitos definidos na norma internacional ISO/IEC 27002:20131.

1. Principais conclusões

A classificação da maturidade da segurança dos sistemas de informação do IFAP, com base no modelo CMM – Capability Maturity Model – corresponde ao nível "(3) – procedimento integrado" (numa escala de 0 a 5), considerando a existência de normas e a implementação dos respetivos procedimentos.Não está totalmente implementada a proposta para o plano de continuidade do negócio. Esta lacuna é preocupante tendo em conta a expressão financeira dos pagamentos efetuados por esta entidade que, no âmbito do FEAGA e FEADER em 2014, ascenderam a M€ 1.387.O Instituto também dispõe de um plano de recuperação de desastres (Disaster Recovery Plan) que não foi testado e implementado, tornando a situação dos sistemas de informação ainda mais crítica.O centro de dados inclui uma grande quantidade de máquinas que estão descontinuadas (sem garantia e assistência) ou em vias de descontinuidade, cuja substituição está contemplada no Plano de Continuidade do Negócio para 2015.O IFAP disponibilizou à Agência de Modernização Administrativa (AMA) a informação sobre o espaço livre a obter, para poder realizar uma gestão mais eficaz e eficiente dos seus centros de processamento de dados e implementar os procedimentos de centralização das TIC, assinalados na RCM 12/2012, de 07 de Fevereiro de 2012.O GAU (Gabinete de Auditoria), seguindo as recomendações da IGF, realizou auditoria à segurança em diversas áreas, em conformidade com as melhores práticas de auditoria.Foi dado início ao processo de certificação ISO/IEC 27001:2013O.

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

Implementar o Plano de Continuidade do Negócio (PCN) no médio prazo.Assegurar um plano de recuperação de desastres (Disaster Recovery Plan) para garantir a recuperação da operacionalidade dos sistemas informáticos em caso de ocorrência de um incidente grave que provoque a paragem total do Datacenter.Desenvolver e implementar um sistema de gestão da segurança da informação que permita controlar os custos orçamentais e a aplicação das boas práticas na gestão do negócio, através da deteção de um conjunto de ameaças e respetiva minimização de riscos.Implementar e concluir o plano de atualização de equipamentos do centro de dados, em paralelo com os exercícios de sensibilização e formação.Iniciar os trabalhos de consolidação do número de centros de dados disponíveis no Ministério da Agricultura, tendo em vista reduzir custos com TIC de acordo com a RCM 12/2012, de 07 de Fevereiro de 2012.Prosseguir na realização de auditorias à segurança, em conformidade com as melhores práticas de auditoria, através do GAU (Gabinete de Auditoria).Informar esta inspeção-geral sobre os resultados do processo de certificação ISO/IEC 27001:2013.

(Relatório n.º 971/2015, homologado, por S. Ex.ª Secretário de Estado Adjunto e do Orçamento, em 2015-07-27).