

Sumário Executivo ANOP nº 3/2019

Avaliação da Segurança da Informação

Período: 21/10 a 29/11/2019

Brasília, DF Dezembro, 2019

Empresa Brasileira de Pesquisa Agropecuária Ministério da Agricultura, Pecuária e Abastecimento Assessoria de Auditoria Interna

Sumário Executivo

O que avaliamos

Avaliamos a situação atual da Segurança da Informação na Embrapa ao analisarmos os processos existentes e as ações realizadas, com base nas normas internas e a legislação vigente. Também avaliamos as ações adotadas pela Embrapa para a proteção de dados pessoais.

Conclusão e Recomendações

A situação atual da Segurança da Informação na Embrapa é resultado de um conjunto de processos e ações em curso desde 2009, conduzido de forma descentralizada pelas Unidades, conforme diretrizes das Políticas de Segurança da Informação estabelecidas. O resultado desta avaliação está dividido em quatro aspectos avaliados: existência de políticas e normas internas, estrutura de gestão de segurança da informação, maturidade do sistema de gestão de segurança da informação e ações para cumprimento da legislação de proteção de dados pessoais.

Ao avaliarmos se a Embrapa possui políticas e normas internas de segurança da informação para orientar os gestores e garantir proteção às informações, constatamos a existência de uma política publicada em 2019, porém os normativos necessitam ser atualizados, pois foram elaborados na vigência de políticas de segurança da informação anteriores.

Sobre este arcabouço normativo, recomendamos a revisão para alinhamento às necessidades atuais da Empresa, e também a definição da estratégia de divulgação e suporte aos gestores de informação, dada a atuação direta destes no cumprimento das normas.

Quanto à estrutura de gestão de segurança da informação na Embrapa, constatamos uma estrutura formalmente instituída, mas parcialmente aderente à legislação vigente. Embora se tenha um comitê gestor de segurança da informação formalmente constituído e uma área responsável pela gestão da segurança da informação, o comitê não vem atuando de forma deliberativa nem o gestor está formalmente designado pela Embrapa.

Também recomendamos a nomeação formal de empregado responsável para atuar como figura central e ponto focal das ações de segurança da informação, tendo em vista a determinação legal. Quanto ao comitê gestor de segurança da informação, recomendamos aprovação do regimento interno para assegurar a autonomia de atuação e dar início ao funcionamento dos comitês locais de segurança da informação nas Unidades.

Um ponto forte da estrutura avaliada é a gestão de incidentes de segurança da informação, mais especificamente a atuação da Equipe de Tratamento de Incidentes da Embrapa, que já vem realizando suas atividades conforme a legislação vigente. Recomendamos que os registros de incidentes sejam acessíveis ao gestor de segurança da informação e que as violações de segurança sejam encaminhadas para adoção de ações corretivas e disciplinares cabíveis.

Na avaliação da maturidade do Sistema de Gestão de Segurança da Informação da Embrapa, constatamos um grau de maturidade intermediário ao consolidarmos os resultados de todas as Unidades, e obter um índice médio de 2,95, numa escala em que cinco seria o valor máximo.

Destacamos como ponto forte a política de controle de acesso aos recursos de TI, mais especificamente os sistemas de informação corporativos da Embrapa.

Por fim, ao avaliarmos o cumprimento da Lei Geral de Proteção de Dados Pessoais na Embrapa, constatamos que as ações realizadas até o momento não garantem cumprimento da legislação. Recomendamos estabelecer a estrutura para o programa corporativo de proteção de dados pessoais, os papéis e responsabilidades das áreas da Empresa.

Também é necessário estabelecer estratégia de comunicação para que todos os empregados, colaboradores, fornecedores e parceiros tenham amplo conhecimento sobre quais são as informações tratadas e por quanto tempo serão armazenadas pela Embrapa, além de instituir mecanismos de comunicação com os titulares de dados pessoais.