ISSN 1983-974X
Janeiro / 2020

DOCUMENTOS
270

Plano de Implantação de Segurança da Informação na Embrapa Gado de Corte: Metas de médio e longo prazo

Embrapa

ISSN 1983-974X
Janeiro/2020

Empresa Brasileira de Pesquisa Agropecuária
Embrapa Gado de Corte
Ministério da Agricultura, Pecuária e Abastecimento

DOCUMENTOS 270

Plano de Implantação de Segurança da Informação na Embrapa Gado de Corte: Metas de médio e longo prazo

José Roberto de Souza Freire
Janaína Paula Marques Tanure
Paulo Henrique Nogueira Biscola
Alfredo Ribeiro Pereira
Tales Augusto Gonçalves Alphonse
João Gomes da Costa

Embrapa Gado de Corte
Campo Grande, MS
2020

Exemplares desta publicação podem ser adquiridos na:

Embrapa Gado de Corte
Av. Rádio Maia, 830, Zona Rural, Campo Grande, MS,
79106-550, Campo Grande, MS
Fone: (67) 3368 2000
Fax: (67) 3368 2150
www.embrapa.br
www.embrapa.br/fale-conosco/sac

Supervisão editorial
Rodrigo Carvalho Alva

Revisão de texto
Rodrigo Carvalho Alva

Tratamento das ilustrações
Rodrigo Carvalho Alva

Projeto gráfico da coleção
Carlos Eduardo Felice Barbeiro

Editoração eletrônica
Rodrigo Carvalho Alva

Foto da capa

1ª edição
Publicação digitalizada (2020)

Dados Internacionais de Catalogação na Publicação (CIP)
Embrapa Gado de Corte

Plano de implantação de segurança da informação na Embrapa Gado de Corte : metas de médio e longo prazo / José Roberto de Souza Freira … [et al.]. - Embrapa Gado de Corte, 2020.
PDF (28 p.) : il. color. - (Documentos / Embrapa Gado de Corte, ISSN 1983-947X ; 270).

1. Legislação. 2. Norma. 3.Segurança da informação. 4. Tecnologia da informação. I. Freire, José Roberto de Souza. II. Tanure, Janaina Paula Marques. III. Biscola, Paulo Henrique Nogueira. IV. Pereira, Alfredo Ribeiro. V. Alphonse, Tales Augusto Gonçalves. VI. Costa, João Gomes da. VII. Série.

CDD 658.472 (23. ed.)

Maria de Fátima da Cunha (CRB – 1/2616)

Autores

José Roberto de Souza Freire

Administrador, doutor em Administração, analista da Embrapa Gado de Corte, Campo Grande, MS

Janaína Paula Marques Tanure

Bióloga, mestre em Genética e Melhoramento, chefe-adjunta de Administração da Embrapa Gado de Corte, Campo Grande, MS

Paulo Henrique Nogueira Biscola

Administrador, mestre em Administração, Pesquisador da Embrapa Gado de Corte,Campo Grande, MS

Alfredo Ribeiro Pereira

Engenheiro-agrônomo, mestre em Ciência Animal e Pastagens

Tales Augusto Gonçalves Alphonse

Especialista em Automação e Controle de Processos Industriais

João Gomes da Costa

Administrador, especialista em Gestão de Pessoas, analista da Embrapa Gado de Corte, Campo Grande, MS

Sumário

Introdução

Este plano apresenta as principais ações realizadas e a serem realizadas em médio e longo prazo relacionadas à Segurança da Informação e Gestão da Informação na Embrapa Gado de Corte, compreendendo a sensibilização dos empregados e a identificação de ameaças e vulnerabilidades dos documentos e ativos institucionais.

Geração do conhecimento, mudança tecnológica e inovação têm sido frequentemente associadas às mudanças econômicas e sociais nos diversos países. Por sua vez, o sucesso das empresas depende cada vez mais da efetividade com que incorporam os novos conhecimentos e sua capacidade de inovar. Deter conhecimento tecnológico fomenta a dominação econômica e política de uma empresa e do país, constituindo um patrimônio nacional.

Proteger esse patrimônio nacional é um desafio da Segurança da Informação que visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela empresa. Para fazer frente a esse desafio a empresa necessita encontrar meios que facilitem o processo inovador, bem como exercer uma nova postura junto à sociedade, desenvolvendo a gestão do conhecimento com a segurança da informação. Essas premissas constituem a base da Política de Segurança da Informação da Embrapa.

Quando pensamos em Segurança da Informação, a abordagem precisa ser planejada e programada, sendo premente a formulação de um plano de ação a curto e médio prazo, com o planejamento de ações que subsidie a efetiva implantação da Segurança da Informação na instituição, em seus quatro principais pilares: pessoas, documentos, infraestrutura e tecnologia da informação.

A efetiva implantação da Segurança da Informação em uma instituição como a Embrapa é um desafio complexo, dependente da atuação de uma liderança engajada que mobiliza suas equipes a atuarem de forma colaborativa, para que os resultados e tecnologias possam ser facilmente obtidas e disponibilizadas à Sociedade, atendendo às diferentes necessidades dos cidadãos.

Comitê Local de Segurança da Informação - CLSI

Janaina Paula Marques Tanure – Presidente
Paulo Henrique Nogueira Biscola – Secretário

Membros

José Roberto de Souza Freire
Carlo César Simioli Garcia
Marlene de Barros Coelho
João Gomes da Costa
Elcione Ramos Simplicio
Erno Suhre

Parceria Apoio
Alfredo Ribeiro Pereira
Tales Augusto Gonçalves Alphonse

"O modo como você reúne, administra e usa a informação determina se vencerá ou perderá."

Bill Gates

Missão da Embrapa

Viabilizar soluções de pesquisa, desenvolvimento e inovação para a sustentabilidade da agricultura, em benefício da sociedade brasileira.

Visão

Ser referência mundial na geração e oferta de informações, conhecimentos e tecnologias, contribuindo para a inovação e a sustentabilidade na agricultura e a segurança alimentar.

Objetivo Geral do Plano de Implantação da Segurança da Informação

Estruturar o escopo da gestão da segurança da informação nos processos da Embrapa Gado de Corte, buscando atender os quatros pilares da Política de Segurança da Informação da Embrapa.

Objetivos Específicos

• Apresentar as principais ações realizadas e a serem realizadas em médio e longo prazo relacionadas à Segurança da Informação dos ativos sensíveis da Unidade.

• Estabelecer foco para ações e resultados na Segurança da Informação de processos da Unidade.

Justificativa

A justificativa da elaboração e implantação de um Plano de Ações de Segurança da Informação para uma instituição reside no valor estratégico da informação para a empresa. São pontos críticos para quaisquer instituições sua dependência dos sistemas de informações e conhecimentos, e a falta de critério e definição se essas informações necessitam, ou não, de procedimen-

tos de sigilo para o sucesso do negócio da organização, considerando que a informação é um ativo e precisa de investimentos e equipamentos de apoio.

As vulnerabilidades dos sistemas de segurança da informação estão sujeitas a diversos riscos e ameaças, tais como: incêndio acidental ou intencional, alagamentos, desabamentos, supressão de serviços por falha de energia, queda nas comunicações, pane nos equipamentos, comportamentos antissociais, falta de controle de recursos humanos, ações criminosas e ataques cibernéticos. Devido ao risco inerente e o grande impacto negativo que essas vulnerabilidades podem representar para a Embrapa, devem ser preventivamente trabalhadas medidas de mitigação de riscos para proteção dos ativos da informação da empresa, fazendo uso das ferramentas da Segurança da Informação.

A segurança da informação abrange o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o conhecimento e a tecnologia gerada pela organização, visando que a informação esteja disponível, sempre que necessária, de forma íntegra e com garantia de sua confidencialidade, possibilitando o cumprimento da missão institucional.

É recomendável que os requisitos que norteiam a Política e os Procedimentos de Segurança da Informação sejam definidos tomando por base as normas da ABNT da família ISO 27000, que tratam especificamente dessa temática. Em especial, destacam-se as seguintes normas:

ISSO 27001 – Gerenciamento da Segurança da Informação
ISSO 27033-3 – Segurança em redes de computadores
ISSO 27033-6 – Segurança em redes sem fio
ISSO 27036 – Segurança da Informação no relacionamento com fornecedores

A segurança da informação existe para minimizar os riscos do negócio em relação aos ativos tecnológicos, bem como contribui para a evolução da governança pública dentro do modelo de gestão pública.

O Modelo de Gestão Pública do Governo Federal passa por evoluções constantes resultantes dos feedbacks recebidos das instituições e dos ciclos contínuos de análise de melhoria, contexto no qual a segurança da informação

está imersa. De forma alinhada às melhores práticas de gestão pública nacionais e internacionais, a Embrapa Gado de Corte pauta suas ações dentro do contexto do seu Modelo Integrado de Gestão, composto por 5 pilares norteadores (Figura 1), dos quais a Segurança da Informação é um dos pilares transversais, que permeia todos os macroprocessos da Unidade.

Para seu planejamento e consolidação, a segurança da informação assumem seus 4 componentes que norteiam sua orientação estratégica, fortalecendo esse um modelo inovador, dinâmico, e de visão sistêmica, com foco na gestão por resultados e na melhoria contínua.

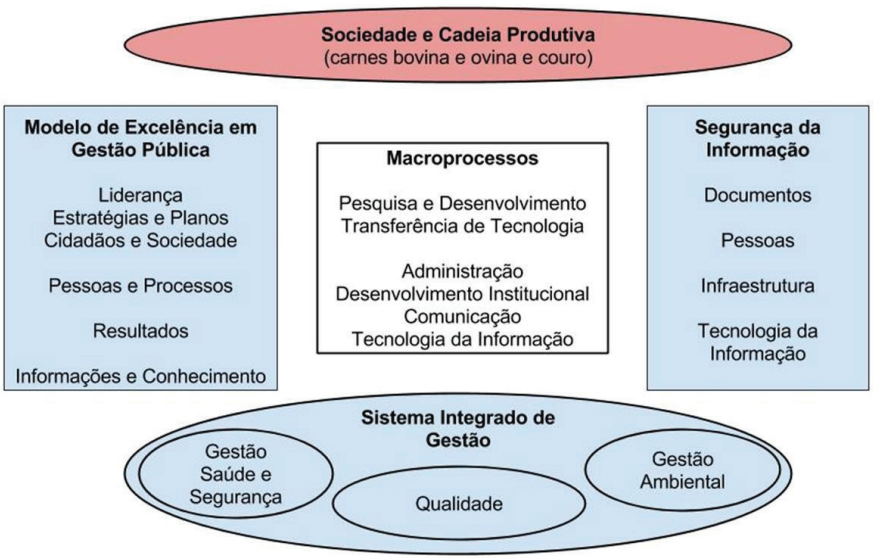

Figura 1. Modelo Integrado de Gestão Embrapa Gado de Corte, Soares et al (2017).

Estratégia para Implantação de requisitos de Segurança da Informação

A estratégia de implantação deve considerar quatro princípios básicos que ajudam nortear as ações em segurança da informação, conforme demonstrado na Figura 2.

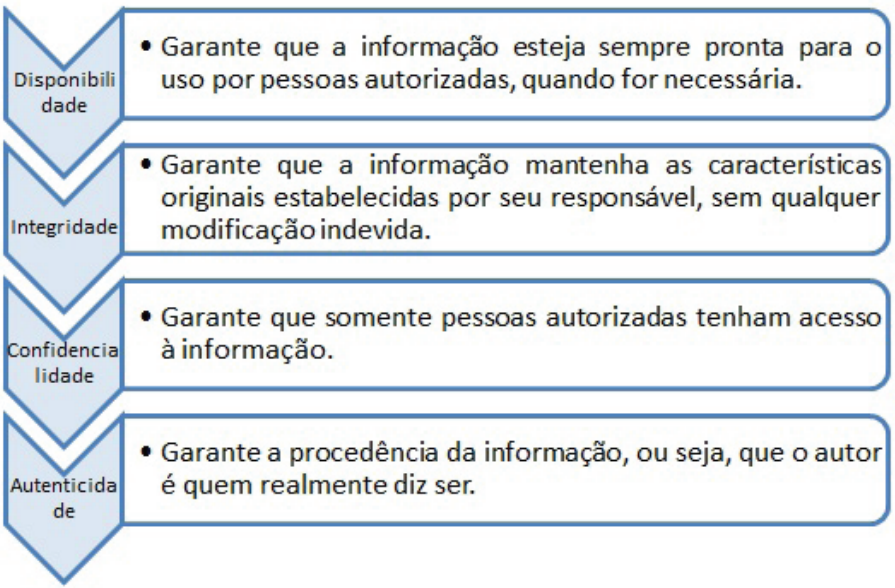

Figura 2. Princípios básicos da segurança da informação, Embrapa, 2016..

Escopo e Metodologia

Como conceito, a Segurança da Informação pode ser entendida como um processo que requer um conjunto de medidas dentro da organização, que visam garantir que a informação esteja disponível sempre que necessária, de forma íntegra e com garantia de sua confidencialidade. A Figura 3 apresenta de forma esquemática os principais elementos que definem o conceito de Segurança da Informação.

Os princípios de segurança da informação adotados na Embrapa Gado de Corte têm por base as diretrizes abrangidas na série de normas ABNT NBR ISO 27000 - que estabelecem diretrizes e princípios gerais para a gestão da segurança da informação em uma organização - e na Política de Segurança da Empresa, Resolução Consad 148/2014, publicada no BCA nº47 de 06.10.2014.

Umas das etapas primordiais para o sucesso da implantação de um plano de segurança da informação é a realização de um diagnóstico abrangente e

consistente em todos os processos da organização. A princípio, realizar um diagnóstico da segurança da informação, é uma forma de realizar uma radiografia de todo o quadro de ameaças e vulnerabilidades das condições de segurança dos ativos daquela organização. Deve-se levar em consideração a análise dos controles básicos das ameaças, e o impacto das vulnerabilidades nos documentos, pessoas, infraestrutura e tecnologia da informação.

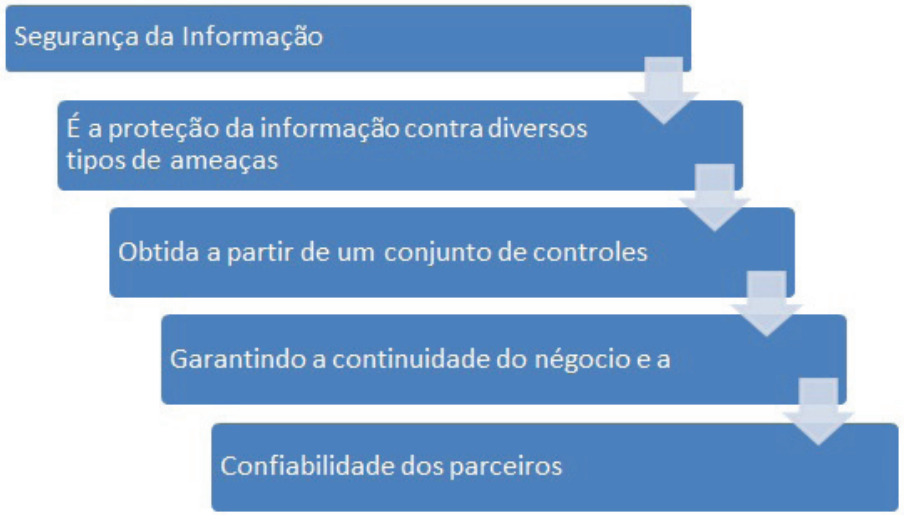

Figura 3. Definição de Segurança da Informação..

As ações previstas e realizadas no Plano de Segurança da Informação da Embrapa Gado de Corte abrangem diretamente as pessoas que trabalham e prestam serviços na organização, bem como seus estagiários, bolsistas e parceiros. Abrange ainda a manipulação de documentos/dados e o acesso à rede de tecnologia da informação.

No que tange à sua aplicabilidade, o plano de segurança da Informação da Embrapa Gado de Corte se aplica tanto aos processos da área meio quanto aos da área fim, e está estruturado da seguinte forma:

1. Política de segurança;

2. Diretrizes da segurança;

3. Identificação de objetos de alvos de proteção;

4. Controle e categorização de documentos /dados;

5. Avaliação de ameaças e riscos;

6. Estabelecimento de procedimentos operacionais padrão;

7. Checklist de área da segurança de informação;

8. Classificação de áreas e instalações;

9. Proteção de áreas e instalações;

10. Gestão de risco de contratos;

11. Gestão de risco em projetos de pesquisa;

12. Monitoramento contínuo.

Deve-se considerar que, para o desenvolvimento desse Plano, as ações devem ser planejadas e realizadas de forma continuada e cíclica, com avaliação de monitoramento (PDCA), para análise crítica do sistema de segurança da informação.

Para assegurar a sua contínua adequação, pertinência e eficácia, as ações do Plano serão coordenadas pelo Comitê Local de Segurança da Informação (CLSI) da Unidade. As ações previstas são de natureza diversa sendo que, para a efetivação de algumas dessas ações, é necessário o dispêndio de recursos orçamentários; para outras serão necessárias melhorias na estrutura de TI, como proteção de segurança de rede e de provedores de serviços à internet; para outras ainda, serão requeridas melhorias na infraestrutura física da Unidade.

Como a segurança da informação nasce nas pessoas e está com as pessoas, é essencial que exista um processo normativo disciplinar na organização de trabalho, caso ocorra alguma violação quanto a SI, onde responsabilidades estejam definidas e atribuídas.

A organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua da segurança da informação, viabilizando a competência necessária às pessoas que

realizam as atividades sob o seu controle, e que afetam o desempenho da segurança.

A Embrapa está subordinada a leis, decretos e normas que estabelecem critérios e requisitos para a gestão de dados e informações na Administração Pública Federal. A Lei das Estatais, em seu art. 8º, determina alguns requisitos obrigatórios relacionados à transparência, dentre os quais se destaca o inciso IV, que determina a elaboração e divulgação de política de divulgação de informações. A Lei de Acesso à Informação, publicada em 2011, com entrada em vigor em maio de 2012, estabelece como um dos princípios a publicidade, como preceito geral, e o sigilo, como exceção.

O decreto da Política Nacional de Segurança da Informação, publicado em dezembro de 2018, e que entrará em vigor em agosto de 2020, estabelece em seu art. 15, inciso III, que os órgãos e as entidades da Administração Pública Federal devem elaborar a sua política e suas normas internas de segurança da informação.

A segurança da informação deve ser pautada em conformidade à Política de Governança de Dados e Conhecimentos da Embrapa. Esta política visa fortalecer os mecanismos de geração, organização, tratamento, preservação, recuperação, divulgação, compartilhamento e reuso dos ativos de informação da Empresa, (RC nº 184 de 04.04.2019; Ano XLV – BCA nº 16, de 05.04.2019). A definição e implementação de procedimentos, estruturas, papéis e responsabilidades é o que norteia e reforça o comprometimento da instituição em garantir a gestão apropriada dos ativos contidos nos seus dados.

Ações de médio e longo prazo de segurança da informação

As ações devem ser desenvolvidas de forma integrada, e permear os quatro componentes que compõem a segurança da informação (Figuras 4, 5, 6 e 7): pessoas, documentos, infraestrutura e tecnologia. São apresentadas a seguir, em linhas gerais, as principais ações a serem desenvolvidas no contexto de cada componente:

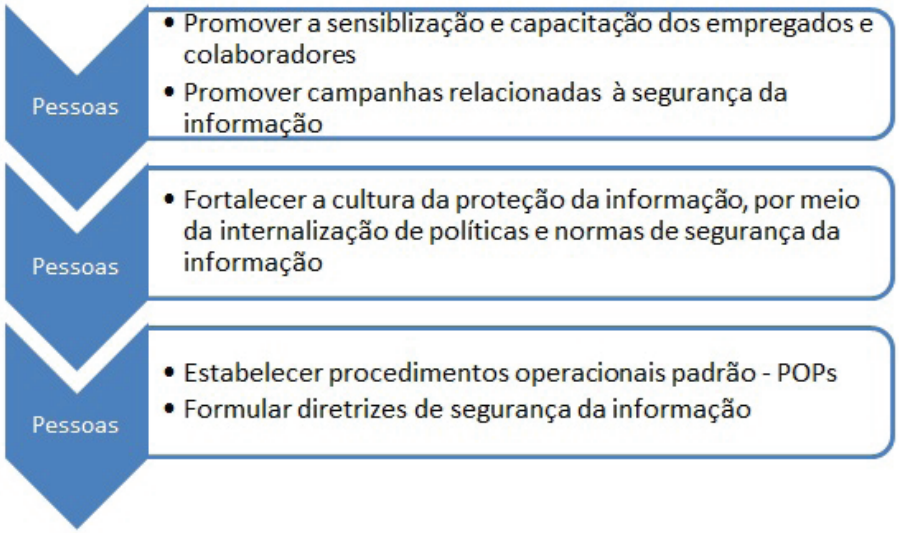

Figura 4. Ações de segurança da informação relacionadas ao componente “Pessoas”.

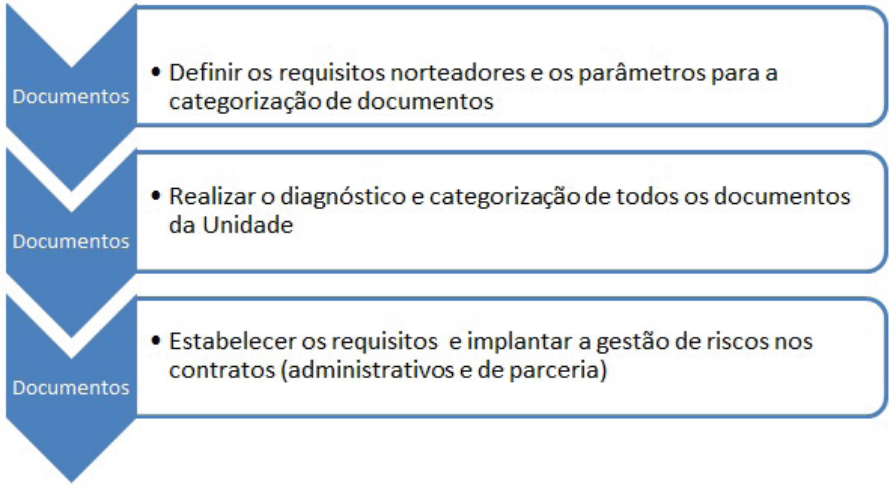

Figura 5. Ações de segurança da informação relacionadas ao componente “Documentos”.

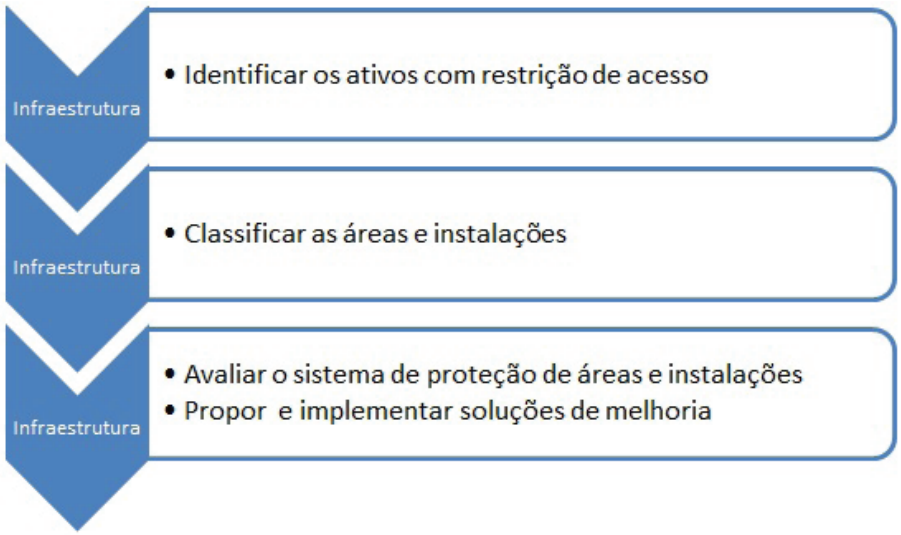

Figura 6. Ações de segurança da informação relacionadas ao componente “Infraestrutura”.

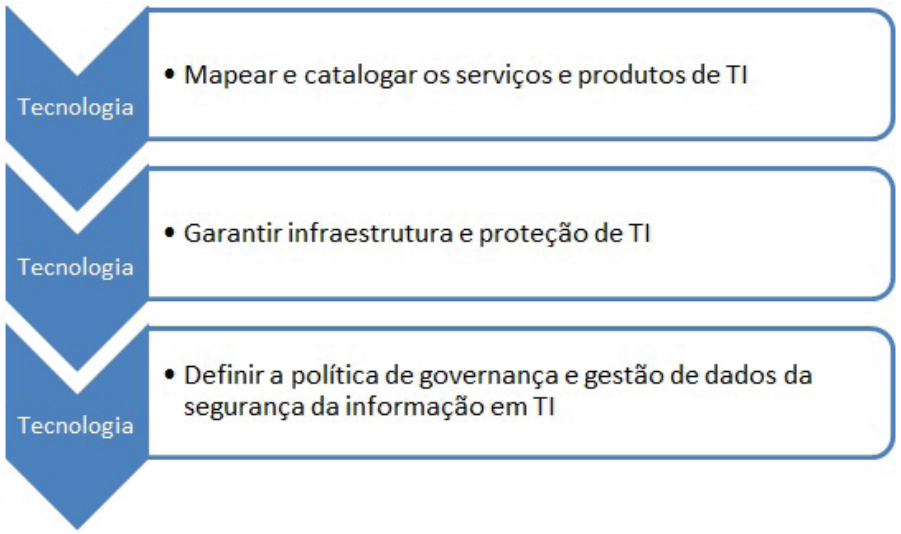

Figura 7. Ações de segurança da informação relacionadas ao componente “Tecnologia da Informação”.

Contexto histórico das ações de segurança da informação na Unidade

A Figura 8 apresenta a linha do tempo com a indicação das principais ações relacionadas à Segurança da Informação desenvolvidas ao longo dos anos, e as futuras ações a serem desenvolvidas na Embrapa Gado de Corte.

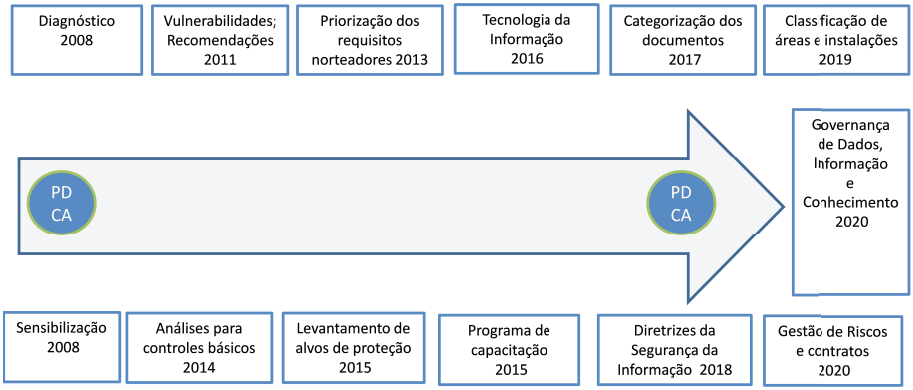

Figura 8. Contexto histórico das ações de segurança da informação.

As ações estruturantes, apresentadas de forma resumida na Figura 9, se constituem como o principal componente do Plano de Implantação da Segurança da Informação da Embrapa Gado de Corte até o momento.

A implantação das ações estratégicas propostas no Plano deve ser coordenada pelo Comitê Local de Segurança da Informação - CLSI, e geridas numa lógica de controle e melhoria contínua de processos.

Esse processo de controle e melhoria contínua deve ser acompanhado por um ciclo de gestão, conforme representado na Figura 10, que envolve o planejamento, execução, monitoramento e avaliação dos resultados das ações.

Figura 9. Ações estruturantes do Plano de Segurança da Informação da Unidade.

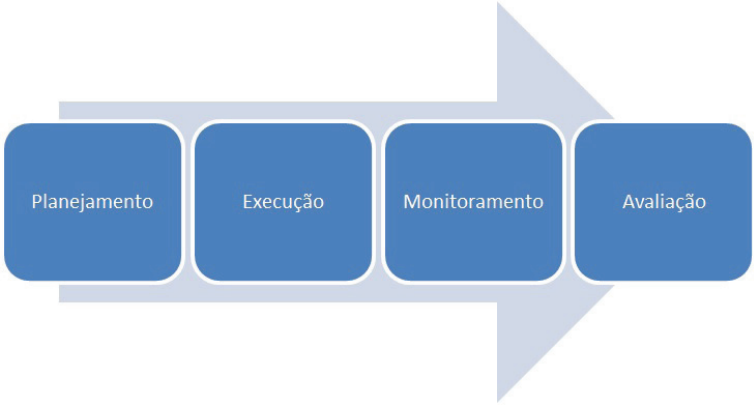

Figura 10. Ciclo de gestão das ações de segurança da informação.

Detalhamento das atividades de cada etapa do Plano de Ação da segurança da informação

Diagnóstico da segurança da informação: levantamento da situação atual em relação aos documentos/dados da Unidade que necessitam de controles relacionados à segurança da informação. O diagnóstico objetiva identificar vulnerabilidades e recomendar ações, procedimentos e controles de segurança para os locais onde são elaborados, manuseados e armazenados dos dados e os conhecimentos sensíveis.

Promoção da sensibilização e capacitação dos empregados e colaboradores: a partir do diagnóstico de segurança da informação, apresentar os resultados aos empregados, para dar conhecimento da situação atual, promover ações educativas, palestras e trabalho em grupo na busca de soluções para as situações futuras.

Identificação dos objetivos alvos de proteção: levantamento dos ativos e suas condições de armazenamento, proteção e distribuição.

Definição das vulnerabilidades e das recomendações: constitui parte do diagnóstico da segurança da informação. Consiste na apresentação de um relatório contendo todas as informações de vulnerabilidades identificadas e as recomendações de ações para mitigação dos riscos. O grau de segurança da informação está intimamente ligado ao ambiente de produção e suas áreas físicas e deve ser um processo preventivo de melhoria contínua. A vantagem nesse procedimento é que a empresa verifique as brechas encontradas e que possa reduzi-las ou eliminá-las antes que possam ser exploradas as suas sensibilidades. Para ser apresentado de forma objetiva, esse diagnóstico pode ser estruturado no formato de tabela, com duas colunas: vulnerabilidades e recomendações.

Levantamentos dos requisitos norteadores: essa fase consiste na definição dos controles básicos de segurança da informação na Empresa, com vistas à definição e priorização de medidas de adoção de controles ainda não existentes ou controles parcialmente implantados. Recomenda-se que seja realizado logo após o relatório de vulnerabilidades e recomendações. Os requisitos norteadores devem ser segmentados nos quatro componen-

tes: pessoas, documentos, infraestrutura e tecnologia da informação e deve ser levada em conta sua priorização. O grau de priorização deve ser estabelecido nos setores e áreas, bem como a criticidade, adotando uma forma de monitoramento contínuo. Necessário se faz uma análise do custo de execução, que deve constar como critério de implantação. A instância corporativa de Segurança da Informação da Embrapa Sede adota um formulário (Figura 11), que pode ser utilizado pelas Unidades, para o levantamento e priorização de requisitos em cada um dos quatro componentes (pessoas, infraestrutura, documentos e tecnologia da informação).

Abaixo, apresenta-se um conjunto de requisitos norteadores que buscam identificar o nível de adoção dos controles básicos de segurança da informação na Unidade relacionados aos componentes Sistemas e Infraestrutura de TI, Infraestrutura Física, Documentos e Pessoas, bem como o nível de criticidade de cada um deles. Na coluna "nível de adoção", pontue de 1 a 4, considerando 1 = Não Adota e 4 = Adota Integralmente. Na coluna "nível de criticidade", pontue de 1 a 3, considerando 1 = Baixo e 3 = Alto. Ressalta-se que não existem respostas certas ou erradas e que essas devem refletir a situação da Unidade.

Escalas de Pontuação

Nível de adoção			
1 = Não Adota	2 = Iniciou procedimento para adotar	3 = Adota parcialmente	4 = Adota integralmente
Nível de criticidade			
1 = Baixo	2 = Médio	3 = Alto	

Categoria	Nº	SISTEMAS E INFRAESTRUTURA DE TI	Nível de adoção	Nível de criticidade	Prioridade
Controle de acesso	1	Controla o acesso à informação e aos recursos e serviços de TI assegurando que somente as pessoas autorizadas tenham acesso liberado.			
	2	Adota procedimento formal para a criação, autorização, remoção e monitoração de contas para acesso aos serviços e recursos de TI.			
	3	Estabelece os direitos de acesso dos usuários com base no princípio do menor privilégio.			
	4	Exige a assinatura de um termo de responsabilidade dos empregados e, onde pertinente, colaboradores, dando ciência das normas de TI, antes de fornecer um login na rede.			
	5	Possui uma política de senhas que assegura a sua qualidade, definindo tamanho mínimo e prazo de validade adequado.			

Figura 11. Levantamento de requisitos norteadores, Embrapa Sede (2016).

Priorização e implantação de ações de segurança da informação em tecnologia da informação: a segurança da informação em TI é um conjunto de ferramentas, estratégias e políticas de segurança que visam proteger os dados da empresa de vários riscos, tais como: proteção e prevenção contra ataques aos sistemas corporativos; prevenção e detecção de vulnerabilidades na área de TI; proteção de informações alocadas em ambientes virtuais; prevenção do acesso de pessoas não autorizadas aos dados corporativos e sensíveis da empresa, e outros. A seguir são apresentadas as ações que minimamente devem ser implementadas no componente de segurança da informação:

a) Inicialmente, realizar levantamento para obtenção de informações a fim de subsidiar melhoria dos processos e normativas internas na área de TI, definindo uma política de segurança de informação em TI;

b) Mapear os recursos de TI disponíveis na Unidade e sob a responsabilidade de cada empregado principalmente: equipamentos, softwares, dados e processos existentes;

c) Realizar a atualização dos sistemas operacionais em computadores clientes e servidores com a ativação de solução de criptografia de disco (BitLocker) e conta única (login e senha) para acesso individualizado a qualquer recurso de TI da empresa;

d) Garantir o acesso físico controlado e monitorado ao ambiente de servidores (Data Center) e salas de telecomunicações; e garantir a implantação e manutenção de mecanismos de controle de incêndio, umidade e temperatura em tais ambientes;

e) Implantar ferramentas de backup automático para garantir cópias de segurança dos arquivos e dados críticos da empresa;

f) Garantir a segurança dos e-mails corporativos, contra ameaças externa e interna, implantando ferramentas para filtrar e reduzir riscos e tentativas de ataques;

g) Implantar sistemática e ferramentas apropriadas para a segregação dos arquivos pessoais dos arquivos da empresa, e garantir a segurança dos dados corporativos;

h) Realizar a categorização e classificação das informações que precisam ser protegidas, bem como garantir a proteção contra vazamento de informações confidenciais, no formato impresso ou digital;

i) Monitorar as entradas e saídas de dados dos sistemas, realizando correlação dos logs gerados em todos os produtos de segurança da empresa;

j) Promover a atualização contínua dos recursos de TI da empresa, incluindo, principalmente, os recursos humanos.

Categorização de documentos, conforme parâmetros de segurança da informação definidos na Unidade: é um dos elementos principais de um processo contínuo de avaliação dos ativos de informação na Unidade, com vistas ao permanente aprimoramento do gerenciamento de riscos, e à garantia da segurança da informação, tendo como referência básica a Norma ABNT NBR 16167:2013. As categorias de segurança devem ser utilizadas em conjunto com análises de vulnerabilidade e ameaças para avaliar os riscos à organização. As categorizações das informações podem ser feitas em três níveis: público, restrito e sigiloso, envolvendo os empregados nessa classificação. É recomendada a elaboração de um Procedimento Operacional Padrão – POP com a definição desses requisitos, de forma a garantir a padronização dos parâmetros de classificação. A categorização dos documentos foi realizada na Embrapa Gado de Corte da seguinte forma:

a) Capacitação básica das equipes dos setores e áreas da Unidade nos conceitos e requisitos da segurança da informação;

b) Durante a capacitação, os empregados identificaram quais os documentos e dados sensíveis ou sigilosos na sua área ou setor;

c) Identificação dos documentos quanto a: produção/registro, marcação, tramitação (expedição e recepção), acesso lógico e acesso físico, armazenamento, reprodução, transporte, transmissão e eliminação.

Os documentos foram classificados em 3 (três) categorias, em conformidade aos parâmetros de categorização do Sistema Eletrônico de Informações – SEI em uso na Embrapa: N1 – documentos que podem ser públicos; N2 – documentos restritos a cargo, grupo ou área; e N3 - documento com acesso específico a pessoas.

Definição e aprovação do Procedimento Operacional Padrão (POP) com as diretrizes da SI aplicáveis à Unidade: o POP é uma descrição detalhada de todas as medidas necessárias para a realização de uma atividade ou processo. O POP em questão define os procedimentos para o tratamento de informações na Unidade e estabelece os critérios para atribuição dos níveis de segurança e acesso às essas informações. A atribuição das categorias de segurança deve ser realizada levando-se em consideração a análise das vulnerabilidades e ameaças, para a correta avaliação e conclusão quanto aos riscos que oferecem à organização.

Classificação de áreas e instalações da Unidade: é a identificação e classificação das áreas e instalações onde se encontram ativos com restrição de acesso. A identificação das áreas deve ser feita de forma detalhada e específica, levando-se em consideração cada sala de uma edificação, a partir do que está mapeado em sua planta baixa. Assim como a classificação de documentos, é recomendável que seja definido e aprovado um Procedimento Operacional Padrão – POP com vistas a definir e uniformizar os parâmetros de classificação de áreas da instituição.

A classificação das áreas e instalações deve ser realizada a partir da categorização dos documentos e dados que cada área possui. Na Embrapa Gado de Corte as áreas podem ser classificadas em:

- **Livre N1:** são áreas e instalações onde não há tratamento de informações, documentos, materiais ou equipamentos com restrição de acesso.
- **Restrita N2:** são áreas e instalações onde há tratamento de informações, documentos, materiais ou equipamentos, com restrição de acesso a determinados grupos ou setores.
- **Restrita N3:** são áreas e instalações onde o acesso aos documentos é exclusivo a quem for atribuída permissão específica.
- **Crítica:** áreas ou instalações de elevada sensibilidade, cujo acesso é restrito somente às pessoas envolvidas nas atividades ali desenvolvidas, mediante prévia autorização.

Proteção de áreas e instalações: consiste na avaliação e aprimoramento do sistema de proteção de áreas e instalações da instituição, levando-se em consideração os seguintes aspectos: barreiras físicas, monitoramento eletrônico e serviços de vigilância patrimonial. O sistema de proteção poderá ser dividido em áreas de segurança interna e externa. As áreas internas podem ser subdivididas em salas de escritórios, sala de equipamentos, corredores de acesso livre e outros. Já as áreas externas podem conter estacionamento, instalações de cabeamento de rede elétrica, sistemas de câmera, gerador de energia e outros.

Proposição de ações específicas para cada área: a partir das informações levantadas no diagnóstico que subsidiou a categorização dos documentos/dados, devem ser estabelecidos planos de ações específicos por área, de forma a sanar as vulnerabilidades e riscos detectados.

No caso da Embrapa Gado de Corte, foram categorizados 126 tipos de documentos, os quais foram classificados em 3 (três) categorias, N1 – documentos que podem ser públicos, N2 – documentos restritos a determinado cargo, grupo ou área e N3 documento com acesso permitido a determinadas pessoas.

A partir desse levantamento, foram estabelecidos planos de ação específicos por setor e sua execução foi inserida no Integro como ação gerencial sob a responsabilidade do setor. Para a construção desses planos de ação, devem ser consideradas todas as informações relevantes, tais como tipo dos documentos sob a guarda do setor e potencial nível de riscos aos dados da empresa. Deve ainda ser definindo o que será feito (qual a ação), porque será feito, quem fará (setor ou pessoa), onde será feito, quando será feito, como será feito e se a ação tem custos, considerando como modelo a Figura 12.

A construção dessa ferramenta pelos próprios empregados do setor, com a condução do CLSI, fomenta uma rica discussão na equipe e permite que as ações e propostas de soluções sejam discutidas conjuntamente e planejadas de forma organizada.

Plano de Ação: Segurança da Informação									
Objetivo:									
Resultado esperado:									
nº	**Documentos***	**Por quê será feito (Potencial nível de danos)**	**O que será feito (atividades e Etapas)**	**Quem fará**	**Onde será feito**	**Quando será feito (Período)**	**Como será feito (como fazer isso? Com que frequencia).**	**Como medir o alcance do resultado**	**Orçamento**
1									
2									

Figura 12. Modelo de plano de ação por área/setor.

Indicadores de ações da segurança da informação

O uso de indicadores torna possível a compreensão da evolução do que se pretende avaliar a partir dos limites, referências ou metas estabelecidas. Na segurança da informação os indicadores estão relacionados com os componentes e a mobilização de diferentes fatores, como pessoas, documentos, infraestrutura física e tecnologia da informação. Na Figura 13 são apresentados alguns indicadores que podem ser utilizados para monitoramento das ações de segurança da informação na Unidade.

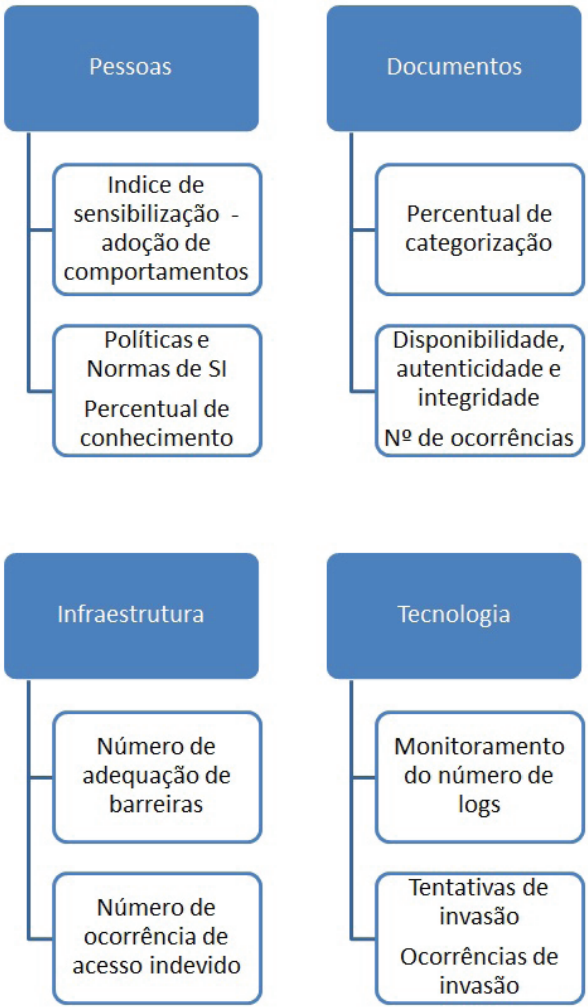

Figura 13. Indicadores de ações da segurança da informação.

Considerações finais

O Plano de Implantação de Ações de Segurança da Informação, a médio e longo prazo, é o resultado de uma série de ações convergentes realizadas e a serem realizadas, com vistas a atender a Política de Segurança da Informação da Embrapa e garantir a segurança das informações e dados críticos da Unidade. Para o sucesso do plano é primordial a sensibilização e envolvimento de toda a equipe, de modo que os setores trabalhem com o componente da segurança

da informação de forma alinhada e com o suporte e orientação da Comissão Local de Segurança da Informação – CLSI, estabelecendo o elo entre a estrutura organizacional setorizada e a Gestão da Unidade.

As atividades previamente programadas das ações operacionais devem ser incluídas no plano de trabalho setorizado da equipe ou do empregado, para que os resultados possam ser planejados, monitorados, e conhecidos de toda a equipe.

Todavia, para que o plano de implantação da segurança da informação se constitua em um instrumento contínuo e efetivo de promoção da segurança da informação, é preciso que as iniciativas previstas se concretizem, as ações sejam realizadas e monitoradas e seus resultados continuamente avaliados, de modo que se fortaleça uma cultura de proteção à informação da Unidade.

Cabe ainda ressaltar que a execução das ações previstas no Plano será de responsabilidade dos Setores e Grupos de Pesquisa da Unidade, devidamente empoderados para exercer a função. O CLSI será, portanto, uma importante instância de apoio, facilitação e monitoramento do processo decisório.

Referências

Associação Brasileira de Normas Técnicas (ABNT). ABNT NBR ISSO/IEC 27000. Tecnologia da informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos. Rio de Janeiro: ABNT, 2013.

Associação Brasileira de Normas Técnicas - ABNT NBR 16167:2013 Segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação.

Associação Brasileira de Normas Técnicas (ABNT). ABNT NBR ISSO/IEC 27002. Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão de Segurança da Informação – Requisitos. Rio de Janeiro: ABNT, 2013.

FREIRE, José R. de S., PATSKO, Carlos, H., BISCOLA, Paulo, H. N., TANURE, Janaina P. M. **Boas práticas em segurança da informação**. Campo Grande, MS: Embrapa Gado de Corte, 2018.

PLANO Tático de Segurança da Informação da Embrapa. Brasília, DF: Embrapa, 2015.

Política de Segurança da Informação da Embrapa. Boletim de Comunicação Administrativa, Brasília, DF, ano 40, nº 74, p.13-16, 06 de outubro 2014.

SOARES, Cleber. O., TANURE, Janaina P. M., ANDREU, Maxwell P., BISCOLA, Paulo H. N. Modelo Integrado de Gestão da Embrapa Gado de Corte [recurso eletrônico] / Cleber Oliveira Soares... [et al]. – Campo Grande, MS: Embrapa Gado de Corte, 2017. 56 p. (**Documentos** / Embrapa Gado de Corte, ISSN1983-974X; 228).

Embrapa

Gado de Corte

Embrapa

MINISTÉRIO DA
AGRICULTURA, PECUÁRIA
E ABASTECIMENTO

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL

CGPE 15845