ISSN 1983-974X
Dezembro / 2018

DOCUMENTOS

261

Boas práticas em Segurança da Informação

Embrapa

ISSN 1983-974X
Dezembro/2018

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

DOCUMENTOS 261

Boas práticas em Segurança da Informação

José Roberto de Souza Freire
Carlos Henrique Patsko
Paulo Henrique Nogueira Biscola
Janaína Paula Marques Tanure

Embrapa Gado de Corte
Campo Grande, MS
2018

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 (2018)

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

Boas práticas em segurança da informação / José Roberto de Souza Freire … [et al.].- Campo Grande, MS : Embrapa Gado de Corte, 2018.
PDF (32 p.). - (Documentos / Embrapa Gado de Corte, ISSN 1983-974X ; 261).

1. Informação – segurança. 2. Legislação. 3. Norma. 4. Política. 5. Tecnologia da Informação. I. Freire, José Roberto Souza. II. Patsko, Carlos Henrique. III. Biscola, Paulo Henrique Nogueira. IV. Tanure, Janaína Paula Marques. V. Série.

CDD 658.472

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

Carlos Henrique Patsko

Físico, Mestre em Física, Analista da Agência de Inteligência Brasileira - ABIN, Campo Grande, MS

Paulo Henrique Nogueira Biscola

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

Janaína Paula Marques Tanure

Bióloga, Mestre em Genética e Melhoramento, Chefe-Adjunto de Administração da Embrapa Gado de Corte - Campo Grande, MS

Sumário

Comitê Local de Segurança da Informação - CLSI (2018)

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

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

Apresentação

Para que se possa implementar um ambiente altamente confiável de segurança das informações depende muito da conscientização de todos: empregados, colaboradores e parceiros. Esta tarefa depende de um Gestor com liderança colaborativa e compartilhada com todos os usuários, em que os resultados devem ser facilmente obtidos em informações que atendam às diferentes necessidades dos setores ou áreas.

A organização precisa entender onde a informação está como é transmitida, armazenada e reproduzida, para isso há leis e regras específicas. A partir destas indicações, e depois de conhecer as informações que você tem e onde encontrá-la, será possível tomar decisões sobre o nível de segurança a ser aplicado e categorizá-la conforme os critérios estabelecidos e definidos com os usuários.

Neste contexto, a informação gerada em uma Unidade de Pesquisa é o resultado de muito trabalho, processamento do conhecimento de várias equipes no qual resultam nos ativos tecnológicos da organização, que são apropriados pelas Instituições de Ciências e Tecnologias, Universidades, Indústrias e Parceiros constituindo assim um patrimônio do país.

Essas ações exigem alguns princípios básicos para garantir que essas informações estejam ao alcance de todos quando necessárias e prontas para uso por pessoas autorizadas, sem qualquer modificação indevida, garantindo sua confidencialidade e autenticidade.

A implementação dessas ações contou com participação de mais de cem empregados sensibilizados na segurança da informação e quinze planos de ações de melhorias que exigem um conjunto de medidas dentro da organização. Apresentamos neste Documento nossas experiências e como chegamos até aqui, buscando uma implementação dos princípios da Gestão de Riscos em Segurança da Informação na Embrapa Gado de Corte.

Introdução

O aumento da capacidade de se atender às demandas globais por produtos e serviços tem reconfigurado à função da Pesquisa, Desenvolvimento e Inovação - PD&I - como meio de fortalecimento das competências tecnológicas nacionais e internacionais. Dessa forma, o domínio de fronteiras tecnológicas conflui para a competitividade nacional, uma vez que os conhecimentos gerados nas instituições de pesquisas são transferidos para o setor produtivo, o que, ao longo do tempo, promove uma espiral do desenvolvimento, com geração de riquezas e de poder.

A Embrapa contribui para a geração de riquezas e de conhecimentos em PD&I agropecuário, e a transferência da tecnologia é realizada em diferentes formatos: impressa ou escrita em papel, armazenada e transmitida eletronicamente ou em conversas públicas e individuais, em vídeos ou televisão e nas mídias sociais. Os valores dessas informações impactam na riqueza do país, e é um ativo essencial para o negócio em PD&I, portanto deve ser adequadamente protegida.

Atualmente, um dos grandes temores de países desenvolvidos é a segurança. E a primeira ação que as organizações fazem é a contratação de vigilantes, aquisição e uso de equipamentos tecnológicos e programas computacionais de criptografia avançada. Mas, há uma fragilidade na Gestão de Segurança da Informação que é a falta ou deficiência de Capacitação das Pessoas – dos gestores, tomadores de decisões, empregados e colaborados em geral – porque a vulnerabilidade da informação, geralmente vem do ser humano.

A fim de minimizar os riscos a Embrapa em 2014 aprovou a Política de Segurança da Informação e suas Normas – BCA Nº 47, de 6/10/2014 – esses documentos, de cunho estratégico, têm como finalidade definir as diretrizes e condições gerais para a implantação do processo da segurança da informação na Empresa. Com base na orientação da Sede a Embrapa Gado de Corte desenvolveu uma série de medidas na área de Segurança da Informação que serão relatadas neste documento.

Esse Documento traduz o que a Embrapa Gado de Corte vem desenvolvendo a respeito da Segurança da Informação nos últimos anos, e tem como objetivo repassar informações praticadas na Unidade com a finalidade do cumprimento das medidas que acompanham a implementação das políticas de segurança da informação da Embrapa.

Segurança da Informação – ações realizadas

Para que um documento seja submetido ao regime de restrição de acesso, ele deve ser enquadrado em alguma hipótese legal de sigilo, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, tal como especificado nas hipóteses legais do art. 23 e art. 24 da Lei nº 12.527/2011, Lei de Acesso à Informação (LAI).

Além das informações classificadas – aquelas sensíveis à segurança da sociedade e o Estado – são também de acesso restrito as informações pessoais. Isto é, aquelas que podem expor aspectos da intimidade e vida privada das pessoas a que se referem. Elas se encontram protegidas pelo art. 31 da LAI. Outras hipóteses legais de sigilo se referem a aspectos de segredo empresarial, sigilo industrial, fiscal, bancário, entre outros previstos na legislação nacional.

Informação é um conjunto de dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, que devem ser preservados pelo seu valor de negócio empresarial ou valor pessoal, em benefício da Empresa, do empregado e da sociedade.

Segurança da informação é 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. Uma série de ações foi realizada na Unidade desde a Avaliação do Sistema de Proteção do Conhecimento, conforme pode ser visualizado na Figura 1 em conjunto com as orientações do Comitê Gestor de Segurança da Informação (CGSI).

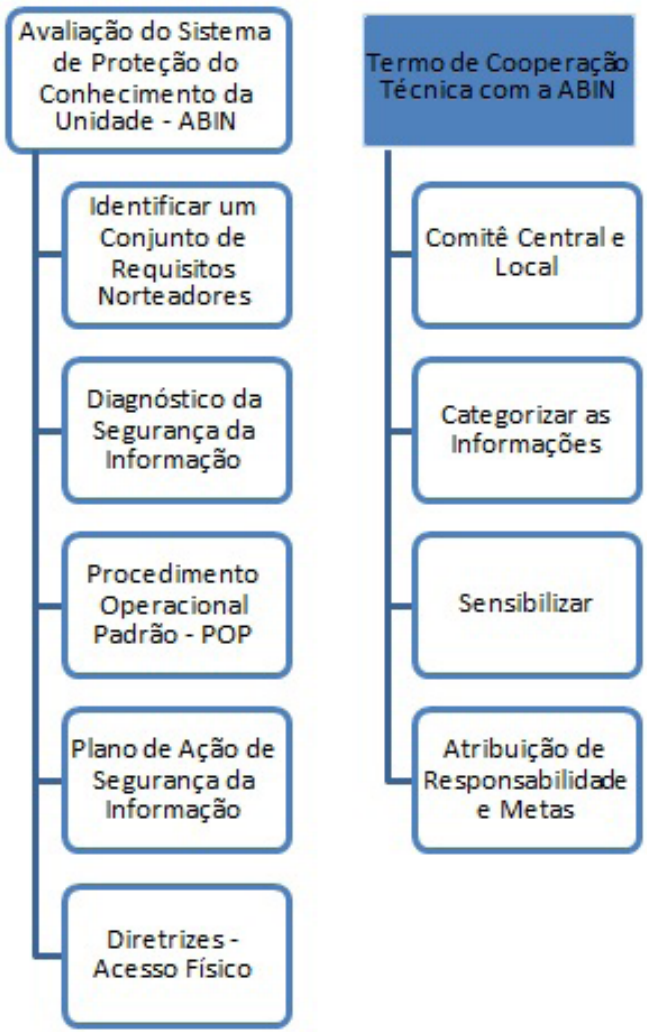


Figura 1. Etapas da atividades realizadas.

Avaliação do Sistema de Proteção do Conhecimento da Unidade

Trabalho realizado em 2009 em conjunto com a Agência Brasileira de Inteligência – ABIN, que resultou em um relatório de avaliação do sistema de proteção do conhecimento da Embrapa Gado de Corte.

Na época, o trabalho teve como objetivo sensibilizar os empregados para a necessidade de salvaguardar os conhecimentos gerados e custodiados pela empresa, definindo as bases do sistema de proteção, alvos e ameaças potenciais, bem como identificando as vulnerabilidades e recomendando algumas medidas e procedimentos de proteção do conhecimento.

Foram realizadas diversas campanhas de conscientização, tendo sido confeccionados brindes institucionais com mensagens alusivas à segurança da informação. Foram realizadas palestras em grupo, e o relatório de avaliação norteou várias ações de segurança da informação no decorrer dos anos, principalmente na área de Tecnologia da Informação.

Identificação de um Conjunto de Requisitos Norteadores

Busca identificar o nível de adoção dos controles básicos de segurança da informação na Unidade relacionados ao componente Infraestrutura física, pessoas, documentos e tecnologia da informação, bem como o nível de criticidade de cada um deles.

Para tanto, foi distribuído um formulário, conforme exemplo apresentado no Quadro 1 de Levantamento de requisitos de norteadores da segurança da informação. Em diversos setores da Unidade para que pudessem identificar o nível de adoção dos controles básicos da Segurança da Informação.

O formulário contém as seguintes escalas de pontuação: na coluna “nível de adoção”, pontue de 1 a 4, considerando 1 = Não Adota; 2 = iniciou procedimento para adotar; 3 = adota parcialmente e 4 = Adota Integralmente. Na coluna “nível de criticidade”, pontue de 1 a 3, considerando 1 = Baixo; 2 = médio e 3 = Alto. Ressalta-se que não existem respostas certas ou erradas e que essas devem refletir a situação da Unidade.

Quadro 1. Levantamento de requisitos de norteadores da segurança da informação – componentes documentos.

Categoria	Nº	DOCUMENTOS	Nível de adoção	Nível de criticidade	Prioridade
Produção	1	Adota os procedimentos de proteção às informações sigilosas estabelecidos pela Lei 12.527 (LAI - Lei de Acesso à Informação).			0
	2	Adota os procedimentos de determinação do grau de classificação do sigilo das informações estabelecidos na Resolução Normativa nº 20 de 03 de junho de 2013.			0
	3	Adota ações de sensibilização dos empregados para o tratamento das informações sensíveis.			0
	4	Adota termo de confidencialidade das informações sensíveis na elaboração do projeto de pesquisa.			0
	5	Adota procedimentos quanto à entrega, utilização, custódia e proteção de documentos que contêm informações sensíveis.			0
	6	Orienta os empregados sobre manter suas mesas ou estações de trabalho limpas, não deixando sobre elas materiais que possam comprometer a segurança de informações sensíveis ou sigilosas.			0
	7	Adota controle de marcação de sigilo nas capas, nos cabeçalhos e rodapés das páginas dos documentos que contenham informação classificada.			0
	8	Adota controle de entrega e uso dos dispositivos de armazenamento portáteis (laptop e mídias removíveis).			0

Fonte: Embrapa Orientações Comitê Gestor de Segurança da Informação - CGSI 2016.

Quadro 2. Planilha de diagnóstico de documentos da segurança da informação.

Identificação Documento/Categoria	Setor	Potencial nível de dano	Nível	Produção/registro	Marcação	Tramitação	Acesso lógico e físico	Armazenamento	Reprodução	Transporte físico	Transmissão	Eliminação
Planilha de Dados de lançamento de matérias secas (pré-secagem)	X	Informações de pesquisa que se tiver acesso indevido podem prejudicar o lançamento da pesquisa	N3	Pesagem de matéria seca e percentuais de variações climática\Planilha no computador	Não são feitas	Via e-mail e Acesso via *Wagara* restrito	Acesso físico e lógico no computador os empregados do Setor, bolsista e pesquisador	Computador do Setor X e no *Wagara* e e-mail do pesquisador do projeto	Não há	Não é realizado .	Via e-mail	Dados históricos não são eliminados até o momento

Fonte: Dados do trabalho

Diagnóstico da Segurança da Informação

Para realizar esse diagnóstico foi realizada uma parceria com a Agência Brasileira de Inteligência – ABIN - para acompanhar e desenvolver a capacitação e categorização de documentos. Utilizando da metodologia de trabalho em equipe, cada setor ou área durante a capacitação tinham como objetivo: identificar, descrever e categorizar os documentos que são gerados e tramitados em seus Setores.

A capacitação atingiu diretamente 65% dos empregados da Unidade, analisando e categorizando 126 (cento e vinte seis) documentos/dados tramitados dentro da Unidade, incluindo empregados das áreas administrativas, laboratórios, apoio a campo experimental, grupos de pesquisa, bem como os Comitês da Unidade.

Os documentos foram categorizados em 3 (três) categorias, N1 – documentos que podem ser públicos, N2 – documentos restritos a cargo, grupo ou área e N3 documento com acesso permitido a determinadas pessoas, utilizando de um planilha com identificação dos documentos, setor, potencial de nível de danos, produção ou registro, marcação, tramitação, acesso lógico e físico, armazenamento, reprodução, transporte físico, transmissão e eliminação.

O formulário pode ser visualizado no Quadro 2, Planilha de diagnóstico de documentos da segurança da informação. Esses documentos foram compilados e apresentados no anexo A do Procedimento Operacional Padrão – POP.

Procedimento Operacional Padrão

Categorização de Documentos em Segurança da Informação

1. OBJETIVO

Estabelecer procedimentos para a atribuição de níveis de segurança e acesso às informações na Embrapa Gado de Corte.

2. CAMPO DE APLICAÇÃO

Este procedimento se aplica às informações públicas e às informações sigilosas não classificadas geradas na Unidade ou por ela recebidas.

3. DOCUMENTOS DE REFERÊNCIA

3.1 Lei de Acesso à Informação (LAI): Lei 12.527/11.

3.2 Decreto 7.724/12, que regulamenta a LAI.

3.3 ABNT NBR 16167:2013 Segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação.

3.4 Resolução Normativa no 19, publicada no BCA no 22 de 03.06.2013.

3.5 Resolução Normativa no 20, publicada no BCA no 22 de 03.06.2013.

3.6 National Institute of Standards and Technology (NIST) Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems, 2018.

3.7 Política de Segurança da Informação da Embrapa (PSI): Resolução Consad 148/2014, publicada no BCA no 47 de 06.10.2014.

3.8 Portaria nº 9, de 15.03.2018, do Gabinete de Segurança Institucional da Presidência da República.

4. FORMULÁRIOS APLICÁVEIS

Não se aplica.

5. DEFINIÇÕES, SIGLAS E ABREVIATURAS

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano a um sistema ou organização.

Ativo: bem controlado pela Embrapa, seja ele tangível ou intangível, que tenha valor para a empresa.

Categorização: processo de atribuir uma categoria aos documentos quanto ao nível de acesso às informações.

Colaborador: pessoa física com vínculo contratual, não empregatício, com a Embrapa (bolsistas e estagiários).

Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a ter acesso.

Classificação: processo de atribuição do grau de sigilo e restrição de acesso (reservado, secreto ou ultrassecreto) a informações consideradas imprescindíveis à segurança da sociedade ou do Estado, nos termos dos artigos 23 e 24 da LAI.

CLSI: Comitê Local de Segurança da Informação é constituído por representantes de diversos setores/grupos autorizados pela Administração; responsável por coordenar, promover e acompanhar as estratégias corporativas da Gestão de Segurança da Informação e das demais iniciativas relativas à segurança da informação.

Criticidade: grau de importância dos ativos para a continuidade do processo de produção da Embrapa.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato.

Grupo de acesso: pessoas, setores/grupos autorizados a ter acesso a uma determinada informação.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação Pessoal: informação relacionada aos dados pessoais, relativos à intimidade, vida privada, honra e imagem.

Informação Pública: refere-se à informação que não sofre restrição legal de acesso.

Informação Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da

sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Informação Sigilosa Classificada: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado nos termos da LAI.

Informação Sigilosa Não Classificada: aquela submetida temporariamente à restrição de acesso público, em razão de fundamento legal específico (sigilo de informações pessoais, sigilo fiscal, sigilo bancário, sigilo empresarial, sigilo de documentos preparatórios).

Integridade: atributo da informação que se encontra completa e que não sofreu nenhum tipo de dano ou alteração não autorizada, não documentada ou acidental.

Necessidade de conhecer: condição pessoal inerente à função ou atividade, indispensável para que o usuário tenha acesso a dados ou informações sigilosas.

Parceiro: pessoa física ou jurídica que mantém com a Embrapa uma relação com atividades específicas ligadas ao desenvolvimento de pesquisa, desenvolvimento e inovação, mas que não é empregada, colaboradora ou prestadora de serviço da empresa.

Prestador de Serviços: pessoa física ou jurídica que mantém com a Embrapa uma relação contratual (contrato de prestação de serviços) de natureza laboral, sem vínculo empregatício, visando à execução de tarefas específicas ligadas ao apoio à gestão da Unidade.

Proprietário da Informação: empregado responsável pela geração do documento ou destinatário que recebeu o documento. Tem como atribuição assegurar que a informação esteja adequadamente categorizada conforme Anexo A.

Risco: medida do quanto uma organização é ameaçada por uma circunstância ou evento. O risco depende dos impactos adversos que decorreriam da circunstância ou evento e da probabilidade de que a circunstância ou evento ocorram.

Rotulação: registro da categoria atribuído ao documento.

Segredo industrial: um subconjunto de informações confidenciais e representam uma forma de propriedade intelectual, trata-se de proteção de dados de desenvolvimento de pesquisa, com caráter de temporalidade indefinida.

Segredo Empresarial: um subconjunto de informações confidenciais e representam um potencial de valor econômico a partir de sua divulgação.

Sensibilidade: grau de importância atribuído pela Embrapa aos seus ativos com o propósito de dar segurança adequada à informação.

Tratamento da Informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Usuário: pessoa autorizada a interagir com a informação.

Visitante: pessoa física sem vínculo contratual direto ou indireto com a Embrapa.

Vulnerabilidade: condição que, quando explorada por alguém com má intenção ou por descuido, pode resultar em uma violação de segurança.

5.1 Siglas

ABIN: Agência Brasileira de Inteligência

ABNT: Associação Brasileira de Normas Técnicas

CGU: Controladoria Geral da União

CLSI: Comitê Local de Segurança da Informação

LAI: Lei de Acesso à Informação (Lei 12.527/11)

NBR: Norma Brasileira

PSI: Política de Segurança da Informação

SEI: Sistema Eletrônico de Informações

SI: Segurança da Informação

6. PROCEDIMENTO

6.1 Este POP trata das informações públicas e das informações sigilosas não classificadas.

6.2 A categorização das informações é um dos elementos de um processo contínuo de avaliação dos ativos de informação na unidade, com vistas ao permanente aprimoramento do gerenciamento de riscos a SI.

6.3 Os procedimentos de categorização, rotulação e tratamento das informações previstos neste POP têm como referência básica a Norma ABNT NBR 16167:2013 e a Resolução Normativa no 20/Embrapa de 03.06.2013.

6.4 As categorias de segurança se baseiam na estimativa dos impactos que decorreriam de eventos que viessem a atingir a segurança das informações necessárias à unidade para cumprir com sua missão, proteger seus ativos, cumprir com suas responsabilidades legais, manter sua rotina de trabalho e proteger as pessoas.

6.5 As categorias de segurança devem ser utilizadas em conjunto com análises de vulnerabilidades e ameaças para avaliar os riscos à organização.

6.6 A categorização das informações será feita em três níveis:

N1: Informações que podem ser divulgadas publicamente (de maneira ativa pela própria unidade segundo as orientações da CGU para a transparência ativa ou de maneira passiva, quando solicitado).

N2: Quando o acesso aos documentos deve ser restrito a determinados setores/grupos ou cargos. O impacto decorrente de perda de segurança da informação (ou seja, de perda de confidencialidade, autenticidade ou disponibilidade) nesse caso seria significativo, podendo resultar em prejuízos aos ativos, às pessoas, às finanças ou à imagem da unidade. Os prejuízos às pessoas incluem, neste caso, danos decorrentes da perda de privacidade das informações pessoais protegidas por lei.

N3: quando o acesso aos documentos é exclusivo às pessoas a quem for atribuída permissão específica. Cada documento N3 tem um rol de usuários credenciados. O impacto decorrente de perda de segurança da informação (ou seja, de perda de confidencialidade, autenticidade ou dis-

ponibilidade) nesse caso seria grave, podendo resultar em prejuízos consideráveis aos ativos, às pessoas, às finanças ou à imagem da unidade. Os prejuízos às pessoas incluem, neste caso, danos decorrentes da perda de privacidade das informações pessoais protegidas por lei.

6.6 Documentos que contêm dados pessoais somente poderão ser acessados mediante consentimento do titular; para o cumprimento de obrigações legais aos trâmites administrativos da Instituição; em razão do exercício regular de direitos em processo judicial, administrativo ou arbitral; ou para a tutela da saúde, esse último por profissionais da área de saúde.

6.7 A categorização dos documentos físicos ou digitais produzidos na unidade deve ser feita pelo(a) empregado(a) responsável pela sua geração. O procedimento será feito com base em tabela no anexo A deste POP. Casos omissos devem ser levados à consideração do superior imediato e comunicados ao CLSI através do e-mail cnpgc.clsi@embrapa.br com vistas a atualizar a tabela.

6.8 A categorização dos documentos físicos ou digitais produzidos fora da unidade deve ser feita pelo(a) empregado(a) destinatário(a) desses documentos. O procedimento será feito com base em tabela no anexo A deste POP. Casos omissos devem ser levados à consideração do superior imediato e comunicados ao CLSI através do e-mail cnpgc.clsi@embrapa.br com vistas a atualizar a tabela.

6.9 A categorização das informações em nível N2 será revisada pelo seu proprietário assim que se alterarem as condições que determinaram essa classificação.

6.10 Entregar ao CLSI somente as informações necessárias para análise e definição da categoria de segurança adequada ao documento, seguindo o procedimento do item 6.5.

6.11 A categorização das informações em nível N3 será revisada conjuntamente pelo proprietário e pelo CLSI assim que se alterarem as condições que determinaram essa classificação.

6.12 Documentos físicos e digitais categorizados como N2 ou N3 devem ser rotulados.

6.13 Nos documentos categorizados como N2 ou N3 deve ser inserido “reprodução, publicação ou retransmissão somente com autorização do proprietário do documento”.

6.14 O rótulo deve ser visível no cabeçalho da primeira página dos documentos físicos, bem como nas pastas e arquivos físicos que os armazenem.

6.15 Mídias digitais, tais como CDs, DVDs, mídias de armazenamento e outras que permitam o transporte de informações devem ser rotuladas de acordo com o nível de categorização mais alto das informações nelas contidas.

6.16 Cada categoria corresponde a um conjunto indicado de procedimentos de tratamento da informação, que consta do anexo B.

6.17 Nos casos de parcerias devem ser adotados procedimentos de compromisso de manutenção de sigilo, quando forem compartilhadas informações de categoria N2 e N3 - (assinatura de termo de sigilo/confidencialidade) ou indicação expressa, por e-mail, de ciência e concordância com a necessidade de sigilo/confidencialidade.

7. RESPONSABILIDADES

Dos proprietários da informação

a) Proceder à categorização das informações por eles geradas ou recebidas de fora da unidade, e a eles destinadas, de acordo com o anexo A;

b) Informar o CLSI através de e-mail (cnpgc.clsi@embrapa.br) no caso de se identificar necessidade de alterações ou inclusões no anexo A;

c) Seguir os procedimentos prescritos neste POP para o tratamento da informação, conforme o anexo B;

d) Informar o CLSI através de e-mail (cnpgc.clsi@embrapa.br) sobre mudanças que se façam necessárias nos procedimentos para tratamento da informação.

Dos usuários

a) Seguir os procedimentos prescritos neste POP para o tratamento da informação (anexo A ou B);

b) Comunicar ao superior imediato falhas nos procedimentos de tratamento da informação;

c) Informar o CLSI através de e-mail (cnpgc.clsi@embrapa.br) sobre mudanças que se façam necessárias nos procedimentos para tratamento da informação.

CLSI

a) Analisar as demandas de revisão na categorização e tratamento das informações que tenham sido solicitadas, ou que o próprio CLSI identifique como necessárias;

b) Apoiar a Chefia Geral em análise crítica anual do POP, visando à sua atualização.

Supervisores

É de responsabilidade do supervisor do setor garantir o treinamento de todas as pessoas que realizam esse procedimento, previamente à sua execução.

Chefe-Geral

Analisar criticamente este POP junto ao CLSI, a intervalos anuais, para verificação de necessidade de revisão.

ANEXO A: REFERÊNCIA DE CATEGORIZAÇÃO

SPS / GESTÃO CONTRATUAL	Contrato de Termo Aditivo de prestação de serviços com terceirização de mão de obra; Penalidade de Advertência e ou Multa; Contrato de Termo Aditivo de prestação de serviços sem terceirização de mão de obra; Autorização de Pagamento.	Sem restrições de acesso	N1
	Planilha de controle mensal de documentação de empregados terceirizados; Folha de pagamento de empregados terceirizados.	Informação Pessoal Não pública nos termos do artigo 31 da LAI	N3

SGP	Contratos e Convênios de Estágios; Frequência; Solicitação de serviço - aquisição de material, Treinamentos obrigatórios na área de segurança no trabalho e higienização de equipamentos de proteção individual – EPI; Extrato Viagem Internacional; Treinamento Individual/Coletivo; Programação de Férias; Aviso Férias.	Sem restrições de acesso	N1
	Pedidos de Transferência; Pedido de Inscrição de pós-graduação e cientista visitante; Processos de bolsistas e estagiários.	Informação Pessoal Não pública nos termos do artigo 31 da LAI	N2
	Atualização Cadastral; ASO/PCMSO; Avaliação Individual; Requerimento de Progressão/Promoção; Pasta Funcional; Perfil Profissiográfico Profissional – PPP; Comunicação de Acidente do Trabalho--CAT; Declaração / Atestado Funcional; Formulário de Viagens internacionais (papeleta).	Informação Pessoal Não pública nos termos do artigo 31 da LAI	N3
SOF	Todos os documentos	Sem restrições de acesso	N1
SPA	Caderneta de nascimento; Baixa de Semoventes; Relatório de comissões (Inventário e Alienação); GTA e nota fiscal transporte animal.	Sem restrições de acesso	N1
SCEFM	Memorando	Informação Pessoal Não pública nos termos do artigo 31 da LAI	N2

SIPT	Formulário de avaliação de eventos; Relatório de Atividades.	Sem restrições de acesso	N1
	Termo de Referência; Cadastro de clientes; Relatório SAC.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N3
SPAT	Processo de proteção intelectual; Formulário Privilegiabilidade; Nota Técnica; Termos de Cessão Direito Patrimonial; Procurações; MEMO encaminha processo - Chefia.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N2
NCO	Material informativo para campanhas internas; matérias jornalísticas.	Sem restrições de acesso	N1
CCSS	Relatórios dos resultados de diagnósticos e metas; Atas de reuniões; Formulário de controle de coleta de resíduos recicláveis.	Sem restrições de acesso	N1
CTI	Atas; Memorial de Tecnologia; Formulários de exequibilidade.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N3
Pesquisa e Desenvolvimento	Carta; Formulário de Receita indireta; Fluxogramas de tramitação de propostas (SEG, fontes externas); Declarações de proponentes de projetos.	Sem restrições de acesso	N1
	Propostas de projetos; Ficha de avaliação de propostas de projeto.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N2
	Projetos; Relatórios de Pesquisa.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N3

Laboratórios	Dados de produção e características de sementes comercializadas; Dissertações e teses; POP´s de laboratório; Dados meteorológicos.	Sem restrições de acesso	N1
	Folhas de Entrada; Planilhas de dados de experimentos; Planilhas de cálculos e resultados de análises; Dados de produção e características de sementes não lançadas; Dados do Germoplasma; Mapas de controle e identificação de amostras.	Segredo industrial (Lei de Propriedade Industrial 9.279/96)	N3
	Planilhas de controle de consumíveis e reagentes químicos.	Atividade de fiscalização (LAI art. 23, VIII)	N3
CEUA	Formulário de recebimento de projeto para avaliação; Certificado.	Sem restrições de acesso	N1
	Roteiro para análise do parecerista; Resoluções e Orientações; Formulário unificado para solicitação de autorização; Formulário relatório inspeção in loco; Atas de reuniões.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N2
	Cadastro de pesquisador; Termo de consentimento; Termo de sigilo.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N3
CIBIO	Manual de Biossegurança	Sem restrições de acesso	N1
	Laudo de vistoria	Atividade de fiscalização (LAI art. 23, VIII)	N3

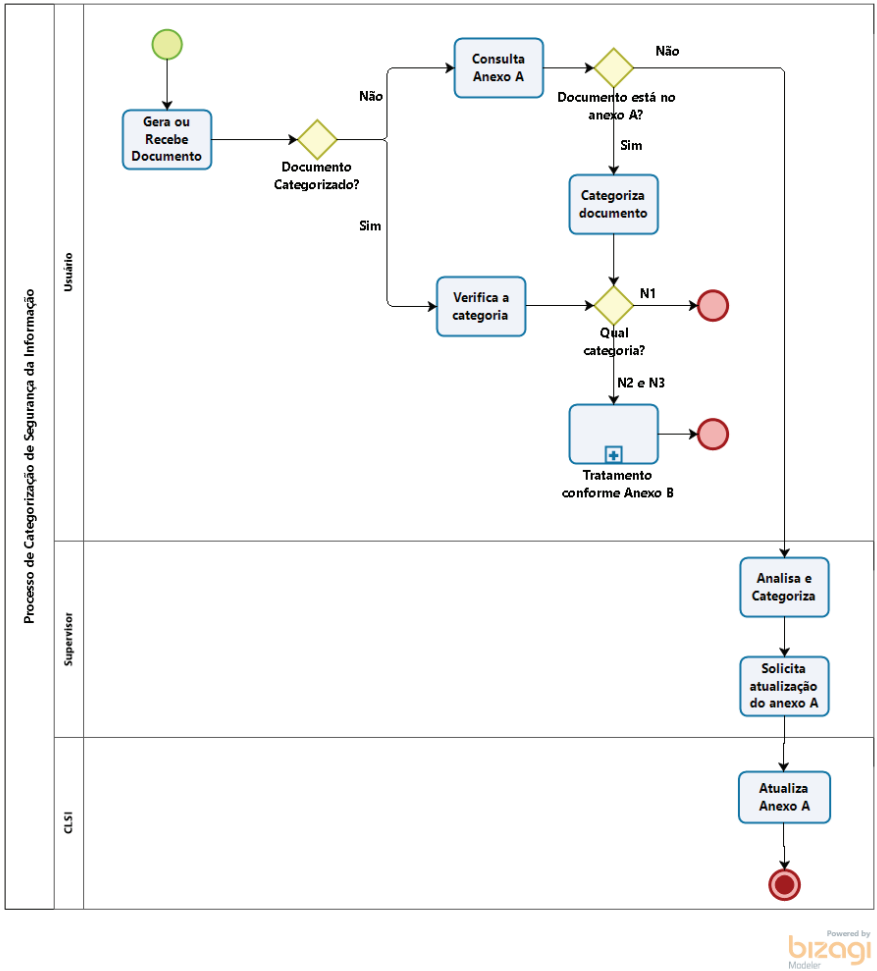
NTI	Carta; Formulário de Requisição de Estação de Trabalho; Inventário de Equipamentos para Leilão; IN04 - Ato de Nomeação / Termo de Referência; Desenvolvimento de Software e Hardware / Implantação / Manual de Usuário do Produto.	Sem restrições de acesso	N1
	Memorando; IN04 - Documento oficializador de Demanda (DOD).	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N2
	Desenvolvimento de Software e Hardware / Demais Documentos.	Segredo industrial (Lei de Propriedade Industrial 9.279/96)	N3
	Infraestrutura / Configuração de Ativos do CPD / Rede de Computadores / Inventário do Parque Tecnológico; IN04 - Análise de Viabilidade, Plano de Sustentação, Estratégia de Contratação, Análise de Riscos.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N3
NDI	Agenda da Unidade; Registro de mudanças de metas administrativas; Processos mapeados; Relatório completo de impactos da UD.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N2
	Ata de reunião do CAE; Relatório executivo do CAE; Banco de Conhecimentos e Tecnologias da Unidade.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N3
UGQ	Documentos padrão.	Sem restrições de acesso	N1
	Documentos físicos gerados pelo UGQ.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N2
	Ajuste metrológico de balanças Marte da série AD.	Sigilo empresarial (Lei de Propriedade Industrial 9.279/96), art. 195, XI-XII	N3

ANEXO B: TRATAMENTO DA INFORMAÇÃO COM RESTRIÇÃO DE ACESSO

Etapa do ciclo de vida	N2	N3
Acesso Físico ou Lógico	Permitido para empregados e colaboradores que atuem nos setores/grupos ou cargos pelos quais o documento deve tramitar.	Permitido para empregados e colaboradores com permissão específica para acesso ao documento. A permissão é concedida pelo proprietário do documento.
Impressão, cópia e armazenamento em papel	Permitido para empregados e colaboradores que atuem nos setores/grupos ou cargos pelos quais o documento deve tramitar.	Permitido para empregados e colaboradores com permissão específica para acesso ao documento. A permissão é concedida pelo proprietário do documento.
Armazenamento em arquivos digitais-rede	No servidor de arquivos da rede da unidade ou no desktop institucional do empregado ou colaborador.	No servidor de arquivos da rede da unidade, com senha de acesso de permissão específica: (Wagara – documentos em desenvolvimento); (Pandora – documentos para armazenamento).
Armazenamento em mídia digital removível (CD, DVD, HD externo, pendrive)	Arquivos devem ser armazenados com criptografia, mídias devem permanecer dentro das dependências da organização.	Não devem ser armazenados em mídia digital removível.
Armazenamento em nuvem (*cloud computing*)	O tratamento em ambiente de computação em nuvem é permitido considerando a legislação vigente e os riscos para a segurança da informação (cf 3.8).	O tratamento em ambiente de computação em nuvem é permitido considerando a legislação vigente e os riscos para a segurança da informação (cf 3.8).

Etapa do ciclo de vida	N2	N3
Transporte Físico	Por pessoa autorizada. O documento deve ser acondicionado de modo a ocultar seu conteúdo (envelope ou pasta).	Por pessoa autorizada. O documento deve ser acondicionado de modo a ocultar seu conteúdo (envelope ou pasta), e com indicação clara do destinatário.
Transmissão por *e-mail*	Com autorização do proprietário e aviso de confidencialidade.	Com autorização do proprietário e aviso de confidencialidade.
Transmissão digital externa (redes de dados, *links*)	Com autorização do proprietário e aviso de confidencialidade.	Com autorização do proprietário e aviso de confidencialidade.
Transmissão de vídeo/ voz; **Transmissão em apresentações**	Permitida a difusão para empregados e colaboradores, desde que autorizada pelo proprietário. Para parceiros deve ser analisada a necessidade de conhecer, adotando quando possível a assinatura de termos ou aviso de sigilo/confidencialidade.	Permitida a difusão para empregados e colaboradores, desde que tenham permissão de acesso. Para parceiros deve ser analisada a necessidade de conhecer, adotando quando possível a assinatura de termos ou aviso de sigilo/confidencialidade.
Eliminação de informação em mídia digital removível	Apagar as informações de modo que sejam irrecuperáveis ou inutilizar as mídias apenas nas áreas da unidade.	Não devem ser armazenados em mídia digital removível.
Eliminação de mídia impressa.	Documento deve ser fragmentado na unidade por empregados e colaboradores que atuem nos setores/grupos ou cargos pelos quais o documento deve tramitar.	Documento deve ser fragmentado na unidade por empregado ou colaborador que tenha permissão de acesso.
Eliminação de arquivos de computador.	Apagar o arquivo de modo que seja irrecuperável.	Apagar o arquivo de modo que seja irrecuperável.

ANEXO C: FLUXOGRAMA DO PROCEDIMENTO DE CATEGORIZAÇÃO SEGURANÇA DA INFORMAÇÃO



Plano de Ação da Segurança da Informação

Modelo do Plano de Ação com objetivo de subsidiar as ações de cada Setor ou Área, desenvolvendo as etapas de elaboração da execução, resultante de um Diagnóstico da Segurança da Informação na Unidade.

Plano de Ação: Segurança da Informação									
Objetivo: elaborar ações preventivas para mitigação de incidentes e problemas de segurança da informação: documentos, pessoas, infraestrutura física e sistemas de TI envolvendo processo de conhecimentos sensíveis e sigilosos, nível 2 e 3..									
Resultado esperado: Plano contendo medidas de segurança da informação para proteção de documentos sensíveis, categorizado como N2 e N3.									
Nº	**Documentos***	**Por que 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 frequência).**	**Como medir o alcance do resultado**	**Orçamento****
1									
2									
3									
4									
5									
6									
7									
8									

* Analisar Formulário (2017) de diagnóstico de classificação de documentos/dados, nível 2 e 3. ** Caso necessário, descrever detalhadamente para ata de registro de preço (aquisição de bens ou serviços).

Diretrizes para Classificação de Áreas Físicas da Unidade

A Segurança das Informações (SI) na unidade depende de um conjunto de medidas que abrangem aspectos relacionados à gestão de pessoas, aos documentos, à Tecnologia da Informação (TI) e à segurança física das áreas e instalações.

Em levantamento dos ativos de informação da unidade, identificaram-se os documentos gerados e/ou custodiados pela Embrapa Gado de Corte, tendo sido elaborado um Procedimento Operacional Padrão (POP) - Categorização de Documentos Segundo Critérios de Segurança da Informação. Esse POP deve nortear os procedimentos de tratamento da informação no âmbito da unidade.

a) Áreas e instalações nas quais o trabalho desenvolvido não envolva a criação ou o tratamento de informações categorizadas como N2 e N3 serão consideradas áreas livres;

b) Áreas e instalações nas quais ocorra a criação ou o tratamento de informações categorizadas como N2 e N3 serão consideradas áreas restritas;

c) As salas com tratamento de informações categorizadas como N2 e N3, deverão ter acesso restrito e na ausência do usuário autorizado deverá permanecer fechada;

d) Áreas e instalações com equipamentos considerados sensíveis em termos de SI pelo setor de TI, ou em termos de biossegurança, serão consideradas áreas críticas;

e) Áreas e instalações restritas e críticas devem contar com meios que possibilitem tratar a informação em conformidade com o anexo B do POP de Categorização de Documentos;

f) Em áreas e instalações restritas, visitantes externos à unidade só devem ser admitidos com prévia autorização do responsável pelo setor, comunicada à portaria geral da unidade;

g) O acesso de visitantes da própria unidade a uma determinada área ou instalação restrita está condicionado à presença, no local, de colaborador que desempenhe suas funções no local visitado;

h) Em instalações e áreas críticas, o acesso de qualquer visitante está condicionado à prévia autorização do responsável pelo local. Os visitantes devem ser devidamente autorizados, identificados e acompanhados;

i) Quando possível, deve ser delimitado um perímetro de segurança em torno de instalações ou áreas críticas, sendo adotadas medidas de monitoramento e detecção de intrusão e previstos procedimentos de respostas a incidentes de segurança;

j) Devem ser adotados procedimentos de sinalização visual das áreas e instalações da unidade, de acordo com a classificação definida.

Os usuários devem possuir acesso às informações categorizadas como N2 e N3 que sejam necessárias, direta ou indiretamente, ao desenvolvimento de suas atividades de trabalho e demais responsabilidades associadas.

Cabe ao Comitê Local de Segurança da Informação (CLSI), no âmbito de suas atribuições, a responsabilidade de contribuir na implantação das diretrizes.

Considerações finais

Segurança da Informação (SI) deve ser objeto de um processo contínuo que envolve elementos de identificação de ativos, análise de riscos e implementação de medidas de mitigação. A participação dos empregados é importante na medida em que a sensibilização quanto à necessidade de mudanças nos procedimentos de tratamento da informação aumenta a adesão às medidas de mitigação de riscos; além disso, se ajustam às prescrições de SI à realidade da unidade, de modo que se prescrevam medidas de proteção factíveis, realistas e adaptadas ao caráter dinâmico da realidade enfrentada por uma instituição de Pesquisa, Desenvolvimento e Inovação (PD&I).

Comumente, um programa de SI busca implementar na organização boas práticas consolidadas em outras instituições. Isso tende a criar um quadro em

que as medidas de proteção são vistas como imposta, sendo muitas vezes pouco adaptadas à realidade da empresa.

A prática adotada buscou estabelecer as bases para uma gestão moderna de riscos de SI na unidade. Iniciou-se com uma capacitação em SI, seguida de um levantamento dos ativos de informação e um diagnóstico dos procedimentos de tratamento de documentos, realizados pelos próprios empregados dos diversos setores da Embrapa Gado de Corte. Em fase posterior, realizou-se um estudo dos normativos da Embrapa, das prescrições legais e de aspectos operacionais do Sistema Eletrônico de Informações (SEI) para elaborar um POP que busca padronizar procedimentos de SI na unidade.

Empregados de todos os setores da unidade foram novamente convidados a analisar os procedimentos de tratamento da informação, propondo medidas de melhorias levando em conta a SI. O POP prevê a necessidade de revisão periódica dos procedimentos, buscando resiliência diante de mudanças na realidade da unidade. A implementação de medidas de segurança da área física é a sequência natural do trabalho desenvolvido, prevista nas metas de 2019.

Referências

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

BRASIL. Decreto 7.724/12, de 16 de maio de 2012, que regulamenta a Lei 12.527, de 18 de novembro de 2011. **Diário Oficial da República Federativa do Brasil**. Poder Executivo, Brasília DF, 16 de maio. 2012. Seção 1, p.1.

BRASIL. Portaria nº 9, de 15.03.2018, do Gabinete de Segurança Institucional da Presidência da República. **Diário Oficial da República Federativa do Brasil**. Poder Executivo, Brasília DF, 19 março 2018. nº 53, Seção 1, pág. 22.

EMBRAPA. Resolução Normativa no 19 e 20, de 03 de junho de 2013. **Boletim de Comunicação Administrativas**, Brasília, DF no 22 de 03.06.2013.

EMBRAPA. Resolução Consad 148, de 02 de outubro de 2014. **Boletim de Comunicação Administrativas**, Brasília, DF, 06 de outubro de 2014.

National Institute of Standards and Technology (NIST) Special Publication 800-37: **Guide for Applying the Risk Management Framework to Federal Information Systems**, 2018.

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

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

Embrapa

Gado de Corte

Embrapa

MINISTÉRIO DA
AGRICULTURA, PECUÁRIA
E ABASTECIMENTO

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL

CGPE 15125