PARA FAZER A DIFERENÇA,

TODO MUNDO CONTA

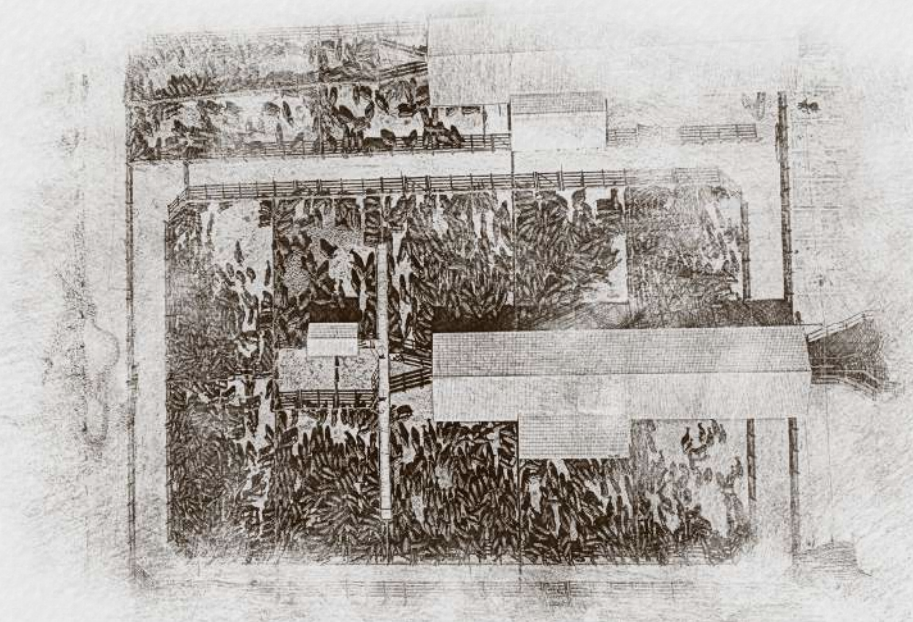
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Junte-se a nós nessa jornada.

JBJ AGROPECUÁRIA

Unidos, somamos atitudes positivas por um futuro melhor.

JBJ AGROPECUÁRIA



Índice

09 1. OBJETIVO

10 2. APLICAÇÃO OU PÚBLICO-ALVO OU ABRANGÊNCIA

10 3. SIGILO DAS INFORMAÇÕES E DE DADOS

3.1. Propriedade Intelectual 11

11 4. PAPÉIS E RESPONSABILIDADES

4.1 Titular de Dados Pessoais 11

4.2 Autoridade Nacional de Proteção de Dados Pessoais ("ANPD") 12

4.3 Alta Direção 12

4.4 Comitê de Compliance 12

4.5 Encarregado pelo Tratamento de Dados Pessoais ou DPO (*Data Protection Officer*) 13

4.6 Gestor da Área de Segurança da Informação 14

4.7 Colaboradores 15

4.8 Terceiros 15

05 5. DIREITOS E REPONSABILIDADES DOS COLABORADORES

5.1 Direitos dos Colaboradores 16

5.2 Responsabilidades dos Colaboradores 17

19 6. DIRETRIZES PARA A PROTEÇÃO DE DADOS PESSOAIS

6.1 Uso das Bases Legais no Tratamento de Dados 19

6.1.1 Base Legal para o Cumprimento de Obrigação Legal ou Regulatória 19

6.1.2 Base Legal para Execução ou Preparação de um Contrato 20

6.1.3 Base Legal do Exercício Regular de Direitos 22

6.1.4 Base Legal do Consentimento 22

6.1.5 Base Legal do Legítimo Interesse 24

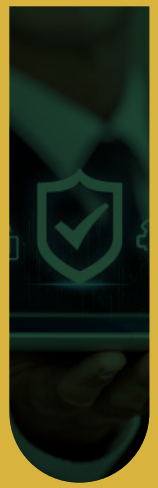
6.2 Tratamento de Dados Pessoais Sensíveis 25

6.2.1 Tratamento de Dados de Crianças, Adolescentes e Idosos 26

6.3 Coleta e Tratamento de Dados Excessivos 27

6.4 Compartilhamento de Dados Pessoais 27

6.5 Retenção e Descarte de 28



Documentos e Dados Pessoais

6.6 Regras para Uso de Celulares e de Aplicativos de Mensagens para Coleta e Compartilhamento de Dados Pessoais 33

6.7 Filmagens Internas e Externas 33

6.8 Uso de Dados Biométricos 33

34 7. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

35 8. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO

8.1. Cadastro de Colaboradores 35

8.2. Uso de Login de Acesso aos Sistemas 36

8.2.1. Uso Individual 36

8.2.2. Criação de Novos Usuários 37

8.2.3. Acesse Somente o que é Necessário 37

8.2.4. Senhas 38

8.2.5. Monitoramento 39

8.3. Regras para Uso de Computadores 39

8.4. Compartilhamento de Informação e Dados 42

8.5. Armazenamento de Arquivos 43

8.6. Uso de E-mail 44

8.7. Normas de Acesso à Internet 45

8.8. Trabalho Remoto e Acesso aos Servidores 47

48 9. DIRETRIZES PARA DESCARTE DE EQUIPAMENTOS ELETRÔNICOS

50 10. GESTÃO DE VULNERABILIDADE

10.1. Gestão de Ativos 52

53 11. CRIPTOGRAFIA

53 12. TREINAMENTOS

54 13. PENALIDADES

56 14. INFORMAÇÕES E DÚVIDAS

57 15. DEFINIÇÕES

15.1 Definições da Lei Geral de Proteção de Dados 57

15.2. Definições de Segurança da Informação 61

63 DECLARAÇÃO

Política de Segurança da Informação e Privacidade

1. Objetivo

A finalidade desta Política de Segurança da Informação e Privacidade é prover diretrizes corporativas para a proteção dos ativos de informações de nossa corporação, de forma a possibilitar o gerenciamento da segurança e da privacidade.

Para fins de esclarecer a melhor utilização dessa política, o material foi dividido em quatro categorias:

INFORMAÇÕES INICIAIS

- Abrangência
- Sigilo das informações
- Papéis e Responsabilidades
- Direitos e Deveres dos colaboradores

ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DADOS

- Princípios
- Diretrizes

ADEQUAÇÕES DE SEGURANÇA DA INFORMAÇÃO

- Princípios
- Diretrizes

INFORMAÇÕES

- Treinamentos
- Penalidades
- Informações e dúvidas
- Definições

Posto isto, o não cumprimento desta é passível de punição. O colaborador deve ser um parceiro da segurança e privacidade da informação para o sucesso desta empreitada.

2. Aplicação ou Público-alvo ou Abrangência

Este Procedimento se aplica a todos que fazem parte da JBJ Agropecuária - Presidência, Diretoria e demais colaboradores. Os preceitos contidos nessa Política também devem ser esperados dos principais fornecedores e outros parceiros de negócios essenciais ao desenvolvimento dos negócios da JBJ.

3. Sigilo das Informações e de Dados

Cada usuário, colaborador, funcionário e/ou fornecedor que gere ou tenha acesso as informações e dados da JBJ, classificadas como confidenciais ou sensíveis, seja por meio tecnológico ou manual, concorda integralmente com esta Política, comprometendo-se a manter máximo sigilo em relação às informações e dados que utiliza ou tem conhecimento.

O descumprimento dessa Política provocará de acordo com a gravidade, além de penalidades internas, possíveis processos judiciais.

3.1. PROPRIEDADE INTELECTUAL

Todas as informações desenvolvidas na prestação de serviços para a JBJ são de sua única e exclusiva propriedade intelectual, sendo seu compartilhamento a terceiros, sem a devida autorização, falta grave passível de punição nos termos desta política.

Eventual requisição de informações por parte de autoridades públicas somente serão cumpridas após a devida validação pelo corpo jurídico e aprovação da Diretoria.

Lembrando que a comunicação com a ANPD deverá ser feita pelo DPO/ Encarregado pelo tratamento de dados.

Na hipótese de expedição de mandado de busca e apreensão de qualquer ativo da JBJ, o colaborador encarregado pelo atendimento deverá exigir a presença de um advogado da empresa, não assinando qualquer documento sem a devida orientação jurídica.

4. Papéis e Responsabilidades

4.1 DADOS PESSOAIS

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, sendo de responsabilidade dos titulares o fornecimento de informações corretas e precisas.

4.2. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS (ANPD)

Órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD e demais legislações correlatas em todo o território nacional.

4.3. ALTA DIREÇÃO

Composta pela Presidência e Diretoria da JBJ Agropecuária que tem a responsabilidade de assegurar que esta política esteja em conformidade com os objetivos estratégicos da empresa, bem como assegurar os recursos necessários para que os resultados pretendidos sejam alcançados. Além disso, a Alta Direção desempenha papel de importante valor no processo de melhoria contínua da gestão da segurança da informação e privacidade ao analisar criticamente e validar as ação desenvolvidas pela empresa.

4.4. COMITÊ DE COMPLIANCE

Composto por membros designados pela Presidência, o Comitê de Compliance atuará em conjunto com o encarregado pelo tratamento de dados pessoais na gestão das medidas adotadas pela JBJ para garantir a segurança da informação e privacidade.

Assim, o Comitê de Compliance irá aprovar o mapeamento de riscos e o plano de ação a ser implementado para promover as adequações da JBJ à LGPD, participará da conscientização dos colaboradores quanto aos novos processos a serem implementados, reportará o andamento das ações programas para a Alta Direção e apoiará o Encarregado no processo de resposta aos titulares de dados e aos órgãos públicos, incluindo a Autoridade Nacional.

Qualquer ato ardiloso, enganoso, de má-fé, com o intuito de lesar ou desvirtuar informações, dados ou fatos para obter benefícios indevidos, ou ainda para o não cumprimento de determinado dever.

4.5. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS OU DPO *(DATA PROTECTION OFFICER)*

Em conformidade com a Lei Geral de Proteção de Dados, a JBJ indicará um colaborador ou terceiro especializado para atuar como canal de comunicação entre a JBJ, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O e-mail de contato do Encarregado pelo tratamento de dados pessoais será divulgado publicamente nos websites www.jbjagropecuaria.com.br e www.jbjagropecuaria.com.

Cabe ao Encarregado pelo tratamento de dados:

i. Receber as reclamações e comunicações dos titulares de

dados, prestar esclarecimentos e adotar providências necessárias para atender as solicitações;

ii. Receber comunicações da autoridade nacional (ANPD) e adotar providências necessárias para atender as solicitações;

iii. Orientar os colaborados e demais contratados a respeito das práticas a serem tomadas em relação à proteção e privacidade das informações, em especial dos dados pessoais;

iv. Executar as demais atribuições determinadas pela JBJ ou estabelecidas em normas legais complementares.

4.6. GESTOR DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Profissional especializado com capacidade técnica para atuar em conjunto com o Encarregado de Proteção de Dados visando o estabelecimento de medidas técnicas e administrativas para garantir a segurança da informação e privacidade dos dados da JBJ.

Reportará ao Comitê de Compliance todas as atividades realizadas e/ou necessárias para que a JBJ esteja em conformidade com as melhores práticas de mercado no que tange a proteção de dados.

4.7. COLABORADORES

Todos os colaboradores da JBJ e empresa afiliadas. Direta ou indiretamente, todos os colaboradores da empresa possuem acesso a informações internas, assim, possuem a responsabilidade de lidarem com as mesmas de forma ética e respeitando as orientações que constam nesse documento.

4.8. TERCEIROS

São todos os clientes, fornecedores, prestadores de serviços, parceiros de negócios que fornecem dados ou tratam dados em nome da JBJ. Aqueles que fornecem dados têm a obrigação de transmitirem informações claras e precisas que serão recebidas e tratadas pela JBJ como verdadeiras. Aqueles que tratam dados em nome da JBJ devem respeitar as orientações específicas estabelecidas em contrato e garantir a segurança e a privacidade de todas as informações compartilhadas.

5. Direitos e Reponsabilidades dos Colaboradores

5.1. DIREITOS DOS COLABORADORES

É direito de todos os Colaboradores:

- Acesso e uso de recursos de Tecnologia da Informação e materiais de consumo de informática necessários para o desempenho de suas funções para a JBJ;
- Login e senhas individuais para acesso a computadores, sistemas e e-mail a serem cadastrados junto ao Departamento de Tecnologia da Informação;
- Acesso a informações e à internet para a realização de suas atividades funcionais;
- Solicitar e receber suporte técnico do Departamento de Tecnologia da Informação.

5.2. RESPONSABILIDADES DOS COLABORADORES

É dever de todos os Colaboradores:

- Cumprir fielmente a Política de Segurança da Informação e Privacidade;
- Buscar orientação de gestores em caso de dúvidas relacionadas à segurança e privacidade da informação;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizadas;
- Não compartilhar senhas de uso pessoal;
- Zelar e assegurar que os recursos de tecnologia da informação e materiais de informática à sua disposição sejam utilizados apenas para as finalidades aprovadas pela JBJ;
- Armazenar nos servidores de rede somente os dados que guardem relação com suas atividades funcionais na empresa;
- Controlar o acesso aos recursos de Tecnologia da Informação que estiverem sob sua responsabilidade;
- Devolver todas as informações, recursos e materiais de informática quando deixar de possuir vínculo com a JBJ, abstendo-se de manter cópias na hipótese da legislação assim não o exigir;
- Devolver ao Departamento de Tecnologia da Informação os computadores de propriedade da JBJ sempre que

sair de férias, recesso, licença médica ou qualquer outro afastamento acima de 10 (dez) dias, para que sejam efetuados reparos, configurações, limpeza da máquina, dentre outros;

- Permitir acesso do Departamento de Tecnologia da Informação ao equipamento sempre que se fizer necessário, para fins de auditoria, averiguação de segurança ou para configuração e/ou instalação de softwares;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Cumprir as leis e normas que regulamentem a proteção de dados pessoais;
- Comunicar imediatamente ao DPO/ Encarregado de Proteção de Dados quando do descumprimento ou violação deste procedimento, bem como perda ou roubo de algum equipamento de informática através dos canais de comunicação disponíveis.

6. Diretrizes para a Proteção de Dados Pessoais

Existem atividades diárias da JBJ que exigem o tratamento de dados pessoais nos mais diversos departamentos da empresa e, justamente por isso, todos devem ficar atentos ao manuseio desses dados. Devemos tratar esses dados com cautela, a fim de garantir sua proteção e privacidade.

Qualquer dúvida em relação a tratamento de dados pessoais deve-se recorrer às definições presentes nessa Política.

6.1. USO DAS BASES LEGAIS NO TRATAMENTO DE DADOS

O colaborar que realizar tratamento de dados pessoais durante suas atividades dentro da JBJ, deve se atentar a qual base legal está amparando aquela atividade em específico.

6.1.1. Base Legal para o Cumprimento de Obrigação Legal ou Regulatória

A JBJ está autorizada a tratar dados pessoais sempre que existir determinação advinda de Lei, decretos, resoluções, dentre outras normas legais que obriguem ou autorizem o tratamento de dados pessoais.

Exemplos para a utilização dessa base legal:

- Coleta de dados pessoais para emissão de nota fiscal;
- O compartilhamento de dados dos colaboradores com o INSS;
- Obrigações tributárias e previdenciárias em geral.

6.1.2. Base Legal para Execução ou Preparação de um Contrato

A execução de obrigações contratuais pode trazer a necessidade de se tratar determinados dados pessoais. Posto isto, diante de contratos para aquisição de produtos ou serviços, os dados poderão ser tratados para a finalidade específica do contrato.

O mesmo ocorre para a formalização de contratos. Procedimentos preliminares à formalização poderão ensejar o tratamento de dados pessoais.

Em todo caso, é obrigatório que o colaborador que estiver executando a atividade esclareça ao titular a necessidade e finalidade do tratamento realizado.

Dentro da JBJ Agropecuária, a base legal de execução de contrato é utilizada nos seguintes casos:

i. Contrato de trabalho realizado entre a empresa e os colaboradores;

ii. Contrato de prestações de serviços com assessoria jurídica, consultoria especializada em Compliance e LGPD, empresas de auditoria, empresas de transporte, assessoria ambiental, segurança patrimonial, segurança do trabalho, arquitetura e agrimensura, controle de pragas, empresas de serviços terceirizados e demais prestação de serviços, incluindo a locação de equipamentos;

iii. Contrato para compra de venda de gado;

iv. Contrato para compra e venda de sal mineral, adubo orgânico e cana-de-açúcar ;

v. Contrato para compra de milho, soja, caroço de algodão, silagem, gordura protegida, DDG, promil, gérmen de milho, ureia, micro e macro nutrientes e demais insumos utilizados na alimentação animal;

vi. Gerenciamento de *Firewall* e redes *Wi-Fi*, manutenção de banco de dados, consultoria em infraestrutura de TI; suporte ao ERP Protheus; plataforma de assinatura digital de documentos; sistema de gerenciamento de ponto; e revenda de softwares da Microsoft.

6.1.3. Base Legal do Exercício Regular de Direitos

O tratamento de dados pessoais dentro de processos judiciais, administrativos ou arbitrais é amparado e autorizado pela base legal do exercício regular de direitos.

Seu objetivo é garantir o contraditório, a ampla defesa e o devido processo legal.

Assim, quando houver situações em que determinados dados pessoais poderão servir como ferramenta para o exercício de direito em processos, tais dados poderão ser armazenados para esta única e específica finalidade, observados os prazos prescricionais das ações, quando deverão ser descartados.

6.1.4. Base Legal do Consentimento

O consentimento dos titulares dos dados para autorizar o tratamento de dados pessoais deve ser dado de forma livre, informada, inequívoca e específica. Para isso deve-se observar:

i. O consentimento deverá ser fornecido por escrito por meio de cláusula contratual destacada das demais cláusulas contratuais ou em documento apartado, podendo ser físico ou online;

ii. As informações devem ser dadas de forma clara, objetiva e transparente, de modo a não deixar dúvidas para o titular;

iii. O consentimento deve ser colhido para finalidades específicas do tratamento;

iv. Deve constar a forma e duração do tratamento;

v. Identificação e contato da JBJ e do Encarregado pelo tratamento de dados (DPO);

vi. As responsabilidades dos agentes que realizarão o tratamento;

vii. Os direitos do titular quanto à confirmação do tratamento, acesso, atualização, retificação, dentre outros que se fizerem necessários.

Caso ocorra mudança da finalidade do tratamento, deixando de ser compatível com o consentimento original, o colaborador responsável deverá informar previamente ao DPO/ Encarregado de Proteção de dados para que comunique o titular sobre as mudanças de finalidade e providencie um novo consentimento.

É proibida a solicitação de autorizações genéricas.

6.1.5. Base Legal do Legítimo Interesse

A base legal do legítimo interesse é utilizada para proteger ou promover interesses próprios da empresa. Deve ser utilizada com cautela pela JBJ.

Antes de utilizá-la, deve realizar uma análise para verificar se há expressa motivação da finalidade e necessidade do tratamento que justifique a escolha do legítimo interesse como base legal, bem como a aplicação em uma situação concreta que garanta a especificidade do tratamento. Isso servirá para fundamentar o Relatório de Impacto à Proteção de Dados Pessoais que poderá vir a ser solicitado pela Autoridade Nacional (ANPD).

Ademais, para utilização do legítimo interesse:

i. Somente os dados estritamente necessários para a finalidade pretendida poderão ser tratados, sendo proibido o tratamento de dados excessivos;

ii. Deve-se adotar medidas que garantam a transparência do tratamento, respeitando sempre as legítimas expectativas do titular.

As legítimas expectativas dizem respeito às expectativas de uso e tratamento dos dados no instante em que foram coletados. Diante do contexto de coleta do dado, o titular prevê que os dados poderão ser tratados para a finalidade em questão que utiliza o legítimo interesse para autorização do tratamento.

6.2. TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

O tratamento de dados pessoais sensíveis é permitido por Lei, contudo deve-se ter maior cautela, considerando que eventual incidente de segurança em relação a esses dados poderá trazer consequências mais gravosas aos seus titulares.

Neste caso, deve-se coletar tão somente os dados estritamente necessários para a finalidade do tratamento realizado.

A base legal do legítimo interesse e da execução e preparação de contratos não autorizam o tratamento de dados pessoais sensíveis, sendo necessário substituir pelo consentimento do titular, que deverá ser de forma específica e detalhada, para finalidades específicas do tratamento.

Atualmente, os dados sensíveis tratados na JBJ são:

i. Raça/cor;

ii. Deficiência física;

iii. Filiação sindical;

iv. Informações de histórico de saúde;

v. Informação se possui ou já possuiu mandado eletivo;

vi. Informações de biometria;

vii. Foto da face;

viii. Imagens de DVR.

6.2.1. Tratamento de Dados de Crianças, Adolescentes e Idosos

O tratamento de dados pessoais de crianças, adolescentes e idosos deverá ocorrer da mesma maneira dos dados pessoais sensíveis, sendo autorizado apenas através do consentimento específico e em destaque, dado por pelo menos um dos pais ou pelo responsável legal.

Visando manter a empresa em conformidade com a legislação brasileira de proteção de dados, devemos manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos quanto à confirmação do tratamento, acesso, atualização, retificação, eliminação, dentre outros que se fizerem necessários.

Posto isto, ao colher o consentimento, as informações sobre o tratamento de dados deverão ser fornecidas de maneira

simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal.

Assim, os colaboradores da JBJ deverão consentir, de forma explícita, para que o tratamento dos dados pessoais de seus dependentes (crianças e adolescentes) ocorram, pela JBJ, com o fim de garantir benefícios como plano de saúde, declaração no imposto de renda, licença maternidade, licença paternidade, entre outros.

6.3. COLETA E TRATAMENTO DE DADOS EXCESSIVOS

A empresa adota o princípio da minimização de dados, ou seja, a coleta de dados pessoais deve estar limitada apenas ao mínimo necessário, para cumprir a finalidade proposta no tratamento de dados pessoais a ser realizado, sendo proíbido o tratamento de dados excessivos.

6.4. COMPARTILHAMENTO DE DADOS PESSOAIS

O compartilhamento de dados pessoais com terceiros, será permitido desde que obtido o consentimento de forma livre, informada e inequívoca do titular para a finalidade específica de compartilhamento.

A exceção será apenas para situações em que a legislação nacional exija o compartilhamento do dado. É proibido o compartilhamento de dados pessoais com terceiros com

objetivo de se obter vantagem econômica.

Na JBJ, os dados pessoais são compartilhados com as seguintes instituições: planos de saúde médica e odontológica; Previdência Social; Ministério do Trabalho e Emprego; clínicas de medicina do trabalho; Receita Federal; Ministério da Agricultura, Pecuária e Abastecimento (MAPA; empresas de vale-alimentação, vale-refeição e vale-transporte, seguro de vida; instituições de ensino e CIEE; cartórios de registro civil, tabelionato de notas e cartórios de registro de imóveis; instituições financeiras,; Microsoft; TOVTS; empresas de auditoria independentes e escritórios de advocacia.

6.5. RETENÇÃO E DESCARTE DE DOCUMENTOS E DADOS PESSOAIS

Todo dado pessoal tem um ciclo de vida que deverá ser respeitado. São fases do ciclo de vida dos dados:

i. Coleta: deve observar os princípios da necessidade e finalidade do tratamento;

ii. Processamento: será autorizado desde que enquadrado em algumas das bases legais (vide item 6.1);

iii. Análise: deve observar a finalidade da coleta, bem como propósito legítimo, específico e explícito para o tratamento;

iv. Compartilhamento: deve ser realizado mediante consentimento do titular, salvo se exigido por norma legal;

v. Armazenamento: os dados devem ser armazenados e mantidos até que sua finalidade seja alcançada ou por prazos definidos;

vi. Eliminação: os dados pessoais devem ser descartados após finalizado o tratamento.

A retenção e o descarte deverão observar a seguinte tabela:

ATIVIDADE	PERÍODO DE RETENÇÃO
Documentos Tributários	05 anos a contar da data de emissão do documento
Contrato de Trabalho	Durante o contrato e mais 05 anos após rescisão.
	Exceções: 30 anos para o FGTS e 10 anos para a folha de pagamento e registro de ponto.
Saúde Ocupacional	Durante o contrato e mais 20 anos após rescisão.
Recrutamento e Seleção	**Reprovação:** prontamente assim que encerrar a finalidade do tratamento. **Aprovação:** durante o contrato de trabalho e mais 05 anos após rescisão.

ATIVIDADE	PERÍODO DE RETENÇÃO
Gestão de Viagens	**Colaboradores:** durante o contrato de trabalho e mais 05 anos após rescisão. **Demais:** 05 anos da data da viagem.
Acesso às Instalações Físicas	15 dias após o último acesso.
Sistema de Imagens	15 dias após a gravação.
Dados Biométricos e Informações de Crachá	Durante o contrato de trabalho.
Acesso aos Sistemas (login esenha)	05 anos após o último acesso.
Contratos Gerais	03 anos após o término do contrato.
Contatos Comerciais	01 ano sem nenhum contato, ou prontamente caso manifeste o desinteresse de ser contactado ou revogue o consentimento, caso tenha dado um.
Sites (cookies, endereços de IP, dados de geolocalização)	01 ano após a última atividade ou prontamente diante da revogação do consentimento.
Serviço de Fale Conosco e canal de denúncias	05 anos após o último atendimento.

Processos judiciais, administrativos ou arbitrais autorizarão o armazenamento dos dados além do período de retenção previsto, independentemente do consentimento.

Findado o período de retenção, os documentos físicos que contenham os dados deverão ser destruídos por picotadora e os arquivos digitais deletados dos sistemas e dos computadores e os comprovantes da realização das operações devem ser arquivados como informação documentada.

6.6. REGRAS PARA USO DE CELULARES E DE APLICATIVOS DE MENSAGENS PARA COLETA E COMPARTILHAMENTO DE DADOS PESSOAIS

Primeiramente, cumpre salientar que o celular corporativo que você utiliza é de propriedade da JBJ, sendo um facilitador do seu trabalho. Você é responsável pelo manuseio correto e zelo do equipamento. Assim, qualquer reparo que seja necessário devido ao mau uso deverá ser ressarcido pelo usuário.

O uso dos celulares para o trabalho deverá se restringir aos programas necessários para o desenvolvimento das funções do usuário, sendo terminantemente proibido o uso para fins pessoais.

O tratamento de dados pessoais através de aplicativos de mensagens deve ser a última opção possível e apenas quando não houver outra possibilidade para a realização de coleta e compartilhamento dos dados.

Quando a opção for realizar o tratamento através do aplicativo de mensagens, os dados devem ser transferidos imediatamente para o sistema da JBJ e excluídos do aplicativo.

Fica proibido o acesso às redes de *Wi-Fi* públicas, bem como habilitar bluetooth em locais públicos.

Caso ocorra um furto ou roubo do celular corporativo, o usuário deverá comunicar imediatamente o DPO/ Encarregado de Proteção de Dados e o departamento de Tecnologia da informação para:

i. Realizar o bloqueio de todos os acessos do dispositivo;

ii. Fazer todas as desconexões remotas que forem possíveis;

iii. Solicitar junto aos bancos a desvinculação das contas, se for o caso;

i. Fazer um Boletim de Ocorrência.

6.7. FILMAGENS INTERNAS E EXTERNAS

A JBJ faz uso de filmagens em suas dependências físicas com o interesse único e legítimo de garantir segurança à própria empresa e todos os seus colaboradores.

O acesso às filmagens é limitado ao Departamento de Tecnologia da Informação que faz a gestão de proteção dos dados e da eliminação de dados no prazo estabelecido por esta Política.

6.8. USO DE DADOS BIOMÉTRICOS

A JBJ faz uso de dados biométricos visando garantir segurança na autorização de entrada nas instalações físicas da empresa.

O acesso a esses dados é limitado ao Departamento de Tecnologia da Informação que faz a gestão de proteção

dos dados e a pronta exclusão ao término do contrato de trabalho.

Ainda que a JBJ trate de dados biométricos para interesses legítimos da empresa, todos os colaboradores deverão dar o seu consentimento para o uso desses dados para os fins específicos mencionados.

7. Princípios da Segurança da Informação

As informações são um ativo importante para o desenvolvimento das atividades da JBJ, de forma que a Política de Segurança da Informação e Privacidade tem como premissa maior proteger este ativo de qualquer ameaça, garantindo que a informação possua:

i **Autenticidade:** a informação é fidedigna, é proveniente da fonte anunciada e não sofreu alterações;

ii. **Confidencialidade:** assegura que a informação somente será acessada por pessoas com acesso autorizado;

iii. **Integridade:** garante que a informação é exata e completa;

iv. **Disponibilidade:** garante que a informação estará disponível ao acesso dos Colaboradores autorizados.

Os Colaboradores autorizados, ao adotar condutas e procedimentos descritos nesta política, contribuem decisivamente para as garantias elencadas acima, garantido a salvaguarda das informações.

8. Diretrizes da Segurança da Informação

8.1. CADASTRO DE COLABORADORES

O cadastro de novos Colaboradores deve ser solicitado pelo Departamento de Recursos Humanos junto ao Departamento de Tecnologia da Informação. O segundo, por sua vez, informará ao novo usuário seu login e senhas iniciais de acesso, bem como as instruções básicas de utilização do sistema e troca das senhas iniciais.

A partir do momento que o usuário recebe seu login e

senha, este passa a ser responsável pela segurança e sigilo dos mesmos, bem como de qualquer atividade desenvolvida por sua conta.

O setor de recursos humanos ficará responsável por qualquer atualização e/ou alteração cadastral dos Colaboradores, devendo sempre comunicar ao Departamento de Tecnologia da Informação eventuais mudanças ou desligamento de colaboradores para que sejam realizados as atualizações e os descadastramentos necessários.

Sempre que o usuário sair de férias, recesso, licença médica ou qualquer outro afastamento acima de 10 dias, o departamento de recursos humanos deverá comunicar o departamento de tecnologia da informação que, por sua vez, desativará temporariamente o usuário até que o colaborador retorne ao trabalho.

8.2. USO DE LOGIN DE ACESSO AOS SISTEMAS

8.2.1. Uso individual

É estritamente proibido o compartilhamento de logins e/ou senhas entre os Colaboradores.

Os acessos são monitorados pelo Departamento de Tecnologia da Informação e em caso de compartilhamento de logins e senhas serão tomadas as medidas necessárias para cessar os acessos indevidos e punir os envolvidos. As punições vão desde advertências até demissão por justa causa, dependendo da gravidade e/ou da importância das informações compartilhadas indevidamente.

As ações realizadas, mesmo que por terceiros, utilizando seu login e senha, serão de responsabilidade do usuário, tendo em vista a proibição de compartilhamento acima.

8.2.2. Criação de novos Usuários

Não compartilhe seu login, mesmo que temporariamente. O correto é a criação de um Novo usuário. Caso haja a necessidade de acessar algum novo sistema, entre em contato imediatamente com o Departamento de Tecnologia da Informação.

8.2.3. Acesse Somente o que é Necessário

Acesse somente aquilo que for necessário ao seu trabalho. Caso em seu acesso seja disponibilizado algum módulo que você não necessita para a realização de suas atividades, Comunique Imediatamente o Departamento de Tecnologia da Informação.

Isso evitará acidentes com os dados da empresa e preservará o acesso do usuário.

Lembre-se, você é responsável pelo que faz no sistema, então, atenha-se somente aos acessos necessários, isso evitará que tenha responsabilidades desnecessárias.

Lembre-se, você é responsável pelo que faz no sistema, então, atenha-se somente aos acessos necessários, isso evitará que tenha responsabilidades desnecessárias.

8.2.4. Senhas

Troque constantemente suas senhas de acesso. O usuário poderá trocá-las espontaneamente a qualquer momento. Também, quando se fizer necessário, exigiremos a troca de senhas.

Lembre-se de usar uma senha segura que seja fácil para você guardar, mas difícil de terceiros descobrirem. Não use números sequenciais e evite datas de aniversário.

Combine números e letras para criar uma senha mais segura, o ideal é que contenha no mínimo seis dígitos e caracteres especiais, como por exemplo: !, @, #, $, %, &, *.

Não forneça a senha de acesso a qualquer sistema da JBJ a terceiros, mesmo que seja uma Autoridade Policial ou Judicial. Neste caso, o fornecimento será realizado exclusivamente pelos advogados da JBJ.

A obtenção de login e senha para uso de aplicativos deverá ser solicitada e justificada pelo gestor do usuário ao departamento de tecnologia da informação. O colaborador que assinar o documento de aprovação referente a este procedimento estará concordando com as regras de acesso aos aplicativos. Deverá ser preenchido um formulário (para documentar o ato) que ficará arquivado na pasta do colaborador, contendo a assinatura do usuário e do seu gestor responsável.

8.2.5. Monitoramento

O login que você está utilizando é de propriedade da JBJ que, como tal, reserva-se no direito de monitorar seus acessos ao sistema e, ao utilizá-lo, automaticamente você estará concordando com nosso procedimento e se comprometendo a cumpri-lo e aplicá-lo fielmente.

8.3. REGRAS PARA USO DE COMPUTADORES

Primeiramente, cumpre salientar que o computador que você utiliza é de propriedade da JBJ, portanto, ele é um facilitador do seu trabalho. Você é responsável pelo manuseio correto e zelo do equipamento, assim, qualquer reparo que seja necessário devido ao mau uso deverá ser ressarcido pelo usuário.

Ademais, fica proibido:

i. Realizar qualquer alteração nas características de hardware e software sem prévia autorização do Departamento de Tecnologia da Informação;

ii. Usar, instalar, executar, copiar ou armazenar aplicativos, programas ou qualquer outro material que não esteja devidamente licenciado e previamente autorizado pelo Departamento de Tecnologia da Informação;

iii. Manter no dispositivo músicas, filmes, obras literárias não autorizadas, proteção de tela ou fundo de tela pessoal, arquivos relacionados a fotos impróprias e animações (com exceção de apresentações corporativas).

Cada computador será protegido por dois logins e duas senhas, sendo uma do usuário e outra do administrador. Somente os analistas do departamento de tecnologia da informação têm permissão para acessar como administrador da máquina.

Cada computador (notebook ou desktop) deverá estar equipado com um antivírus e antispyware (spyware são arquivos maliciosos cujo objetivo é roubar dados), para segurança do usuário. A responsabilidade da instalação do antivírus é do Departamento de Tecnologia da Informação.

O uso dos computadores para trabalho deverá se restringir aos programas necessários para o desenvolvimento das funções do usuário, sendo terminantemente proibido o uso para fins pessoais.

Está terminantemente proibido o uso de dispositivos de armazenamento móvel por USB, como *Pen Drives*, *Memory Keys*, HD externo ou qualquer outro meio, com exceção daquelas pessoas que precisam de tais dispositivos como ferramenta de trabalho, e tenham a devida anuência do gerente e/ou diretor da área.

Sempre que se ausentar temporariamente do seu local de trabalhado, o usuário deverá bloquear o computador que estiver utilizando ou realizar logoff. Ao final do expediente deve-se desligar o computador.

Diariamente serão feitas auditorias em todos os computadores com o objetivo de verificação do cumprimento dos itens deste procedimento.

Sempre que sair de férias, recesso, licença médica ou qualquer outro afastamento acima de 10 dias, deve-se devolver o computador ao departamento de tecnologia da informação para que se possa fazer limpeza da máquina, reparos e atualizações de software.

A conexão de computadores particulares utilizando a infraestrutura corporativa é proibida, exceto para consultoria e auditoria externa com autorização do gerente da área.

Caso ocorra um furto ou roubo do computador, o usuário deverá comunicar imediatamente ao DPO/Encarregado de Proteção de Dados e o Departamento de Tecnologia da Informação para:

ii. Realizar o bloqueio de todos os acessos de sistemas do dispositivo;

iii. Fazer todas as desconexões remotas que forem possíveis;

iv. Fazer um Boletim de Ocorrência.

8.4. COMPARTILHAMENTO DE INFORMAÇÃO E DADOS

O Departamento de Tecnologia da Informação só poderá liberar o compartilhamento de arquivos entre departamentos após autorização expressa do gestor do departamento a ser acessado, indicando o nível de acesso e a confidencialidade das informações.

É importante sempre observar a classificação da informação antes de realizar o compartilhamento de qualquer dado da JBJ, seja com os departamentos internos, seja com terceiros.

Assim, ressalta-se que o compartilhamento de dados pessoais deve se restringir somente aos terceiros que possuem contratos firmados com a JBJ com obrigações expressas de cumprimento da LGPD, bem como dos controles necessários para garantir a segurança das informações compartilhadas.

Em caso de dúvidas no compartilhamento de dados, sempre consultar o DPO/Encarregado de Proteção de Dados da JBJ através dos canais de comunicação disponíveis.

8.5. ARMAZENAMENTO DE ARQUIVOS

O armazenamento de arquivos da JBJ deverá ser realizado no servidor de aplicativos, em pastas devidamente organizadas por Colaboradores ou setores. Existirão níveis de acesso e cada usuário acessará somente as pastas do respectivo departamento. O arquivamento no servidor será de competência do usuário e a tecnologia da informação proverá meios para que o usuário tenha acesso ao servidor de arquivos.

Recomenda-se o não armazenamento de arquivos diretamente nos equipamentos uma vez que não poderá ser realizado o backup dos mesmos de forma automática pelo Departamento de Segurança da Informação, o que aumenta o risco de indisponibilidade dos arquivos em caso de dano, furto ou roubo do equipamento.

8.6. USO DE E-MAIL

É proibido o uso de e-mails não corporativos. Somente será permitido o uso dos domínios @jbjinvestimentos.com.br, @jbjagropecuaria.com.br, @beefbistro.com.br, @bbmedical.com.br, @eaglejet.com.br.

Os e-mails corporativos são de uso e propriedade da empresa, portanto não devem ser utilizados para fins pessoais e serão amplamente monitorados.

O tamanho máximo de arquivos anexos é de 14 MB (14.336 Kbytes) para os Colaboradores da Matriz e 10 MB (10.240 Kbytes) para os Colaboradores das demais unidades. Não sendo permitido o envio de arquivos com a extensão ".exe", bem como outras extensões classificadas como de alto risco pela área de Tecnologia da Informação.

A JBJ possui um padrão de assinatura de e-mail, o qual não poderá ser alterado ou ter a inserção de animações ou imagens diversas.

É proibido o uso para troca de spam, piadas, animações, pornografia, dentre outros. Todos esses itens serão tratados como desvios sérios de conduta corporativa, passíveis de punição.

Deve-se ter bastante cuidado com spams, eles vêm em e-mails não solicitados, com mensagens que exploram sua confiança e cujo objetivo é roubar suas senhas de acesso ao home banking. Dessa forma, não abra e-mails que não tenham sido solicitados, e nem e-mails cujo assunto seja estranho, pois podem ser vírus. Para certificar-se de que o endereço ao qual você está se conectando é o mesmo sugerido no e-mail, coloque o mouse, sem clicar sobre o link do arquivo e aparecerá o verdadeiro endereço. Certifique-se que o endereço seja conhecido ou correspondente ao assunto em questão. Em caso de dúvida, contate o departamento de tecnologia da informação.

Por fim, é disponibilizado o serviço Web Mail para ser utilizado sempre que os serviços de correio (Outlook) apresentarem algum problema e/ou o colaborador estiver em viagem.

8.7. NORMAS DE ACESSO À INTERNET

Todo acesso será monitorado e será expressamente proibida a utilização de sites que não correspondam às necessidades das suas funções (jogos, fotos impróprias, batepapo, etc). Serão bloqueados sites de conteúdo impróprio. O acesso a este tipo de conteúdo constituirá falta grave e o infrator ficará sujeito às penalidades cabíveis.

Fica expressamente proibido acessar internet de máquinas ou dispositivos que não pertencem ao seu setor.

O software de comunicação é o Teams da Microsoft, o

software de compartilhamento de arquivos é o SharePoint e o software de abertura de chamados internos é o GLPI. A plataforma de e-mail padrão do Grupo JBJ é o Exchange da Microsoft.

Em casos específicos para atenderem aos interesses da empresa, podem ser concedidas exceções, para utilização de softwares de comunicação, tais como *WhatsApp*, em modo *mobile*, não sendo permitido o uso da versão *WhatsApp Dektop*.

Ressaltamos que o compartilhamento de dados pessoais por esta plataforma somente será permitida nos casos em que os demais softwares corporativos disponibilizados pela empresa não estejam acessíveis pelas partes.

Plataformas de armazenamento de arquivos em nuvem como Dropbox, Google Drive, Mega, entre outros não podem ser utilizados para armazenamento de dados e arquivos da JBJ Agropecuária. Em caso de auditoria interna, os colaboradores serão instruídos a não utilizar estas plataformas pessoais para armazenamento dos dados da JBJ e o compartilhamento será removido pela equipe interna de TI e segurança da informação da JBJ.

Eventualmente, poderá ser concedido acesso à internet por meio da rede wi-fi da empresa a usuário não cadastrado. O acesso deverá ser solicitado ao Departamento de Tecnologia da Informação que avaliará o pedido e disponibilizará o acesso. O usuário temporário ficará sujeito aos termos desta Política de Segurança da Informação e Privacidade.

8.8. TRABALHO REMOTO E ACESSO AOS SERVIDORES

O trabalho e acesso aos servidores de forma remota, serão permitidos após justificativa e autorização do gestor ou diretor do departamento. Por sua vez, o Departamento de Tecnologia da Informação deverá ser informado e continuará realizando o trabalho de monitoramento do sistema.

Todas as regras estabelecidas nesta Política deverão ser observadas durante o trabalho remoto.

O acesso aos equipamentos eletrônicos e sistemas da JBJ deverão ocorrer, preferencialmente, dentro do horário de trabalho. Acessos fora dos dias e horários de trabalho deverão ser exceção e devidamente justificados, considerando que o suporte técnico do Departamento de Tecnologia da Informação se torna mais dispendioso.

O acesso à internet por meio da rede wi-fi que não seja da JBJ será permitido para o trabalho remoto, contudo deverá ser realizado com cautela.

O usuário não deve usar seus laptops em locais públicos e em áreas desprotegidas. Fica proibido o acesso às redes

de wi-fi públicas.

Findada a necessidade de trabalho e acesso remoto, o usuário deve procurar o Departamento de tecnologia da Informação para que seja realizada uma limpeza nas redes wi-fi salvas, dentre outras ações que se fizerem necessárias.

9. Diretrizes para Descarte de Equipamentos Eletrônicos

Havendo a necessidade de descarte de equipamentos eletrônicos de propriedade

da JBJ, o descarte será realizado em conformidade com a Política Nacional de Resíduos Sólidos.

O primeiro passo é verificar a situação em que o equipamento se encontra. Se o equipamento não estiver quebrado e for possível o acesso ao mesmo, deve-se proceder com algumas medidas que visam proteger a informação.

No caso de celulares, recomenda-se desvincular a conta de seu fabricante, apagar todos os dados através de restauração do sistema e retirar o chip.

No caso dos computadores, deve-se proceder com a formatação completa do HD.

Todos os dados devem ser apagados de forma segura.

Isso vale também para dados e softwares licenciados armazenados em mídias de armazenamento móvel (por exemplo, em CD, DVD, pen drive USB, cartão de memória, token de certificado digital, etc., e também em papel). Todos devem ser apagados de forma segura, a mídia deve ser destruída antes de ser descartada.

Recomenda-se a utilização de *softwares* especializados ou a contratação de empresas de consultoria para garantir a não reversão dos dados e impedir o acesso indevido de informações confidenciais e dados pessoais de titulares de dados vinculados à JBJ.

O Departamento de Tecnologia da Informação é responsável por apagar e destruir os dados dos dispositivos móveis.

Realizada a limpeza dos equipamentos, deve-se verificar

junto ao fabricante se eles realizam coleta de aparelhos. Caso não haja coleta pelo fabricante, verificar pontos de coleta na cidade. Caso os equipamentos estejam em bom estado de uso, os mesmos podem ser doados para instituições sociais, conforme definição da Diretoria.

10. Gestão de Vulnerabilidade

A vulnerabilidade consiste na fraqueza dos ativos de tecnologia da empresa que, de alguma forma, podem ser explorados por ameaças. Para combater essas ameaças e minimizar danos, faz-se necessário:

i. Configurar toda a tecnologia corretamente e para isso a JBJ conta com o auxílio do Departamento de Tecnologia da Informação. Todos os Colaboradores ficam proibidos de realizar qualquer alteração nas configurações de ativos que tiverem acesso;

ii. Realizar processos de verificação, que ficará a cargo do Departamento de Tecnologia da Informação;

iii. Realizar testes de intrusão periódicos;

iv. Treinar o Departamento de Tecnologia da Informação;

v. Promover a conscientização de todos os colaboradores e terceiros que possuem acesso aos ativos e sistemas da JBJ.

O Departamento de Tecnologia da Informação deverá atuar junto ao Comitê de Compliance na gestão de riscos e vulnerabilidades aos quais a JBJ está exposta, a fim de mitigar riscos e garantir melhorias à segurança das informações e de dados.

Ademais, o departamento de tecnologia da informação deve estabelecer a prática de receber de fabricantes notícias e atualizações de software, pois é possível que o fabricante promova alguma atualização ou patch para consertar problemas detectados.

A varredura contínua da rede de computadores deverá ser realizada para detecção de endereços de IPs que estão respondendo, portas de comunicações abertas e as versões de software rodando nessas portas. A varredura contínua pode ajudar a descobrir dispositivos vulneráveis e permitir uma correção.

Por fim, a vulnerabilidade pode estar nas pessoas, por isso é fundamental o treinamento quanto a diretrizes dessa Política, bem como simulações, como as de phishing para saber se os colaboradores estão atentos às diretrizes da empresa.

10.1. GESTÃO DE ATIVOS

A gestão de ativos é obrigatória e necessária dentro da JBJ. O Departamento de Tecnologia da Informação manterá um inventário atualizado, o que auxilia na gestão de vulnerabilidades.

Sempre que houver a identificação de qualquer fraqueza, com o inventário de ativos é possível saber onde devemos atuar.

O controle de ativos deverá conter no mínimo:

i. **Ativos de *hardware*** – lista de todos os dispositivos sob a administração do Departamento de Tecnologia da Informação, como, por exemplo, computadores, celulares, *roteadores*, *storages*, *firewalls* e afins, servidores, access point, *no-breaks*, dentre outros que houver.

Com informações como endereço de IP, dados do fabricante, modelo, número de série, dentre outros, e com quem ou em qual departamento os ativos estão alocados.

ii. **Ativos de *software*** – para cada *hardware* a indicação do *software* instalado, com versão atual e data de instalação.

Ainda, faz-se necessário sensor de presença e status de conectividade dos dispositivos na rede.

11. Criptografia

Visando mitigar vulnerabilidade às quais a JBJ pode estar exposta, faz-se necessária a criptografia total de disco dos computadores da empresa com o controle de gerência de chaves, a fim de manter a confidencialidade dos dados.

É de responsabilidade do Departamento de Segurança da Informação estabelecer os critérios que serão utilizados para a criptografia dos dados, sendo necessário o uso da tecnologia para os dados confidenciais e sensíveis.

12. Treinamentos

A JBJ manterá um plano de treinamento para os colaboradores com o objetivo de esclarecer quanto a importância e necessidade da proteção e privacidade das informações, as implicações que as violações trazem tanto para a empresa, quanto para o próprio colaborador, bem como assegurar que as regras, diretrizes e procedimentos

adotados por esta política foram bem compreendidos e que todos saibam quando e como aplicá-las.

Os treinamentos serão realizados periodicamente com a finalidade de se revisar o conteúdo e fortalecer uma cultura de proteção e privacidade da informação através da conscientização contínua.

13. Penalidades

As penalidades vão desde advertência verbal até demissão por justa causa.

O descumprimento desta Política será apurado pela área de Tecnologia da Informação e reportado ao Comitê de Compliance para as devidas providências e aplicações de sanções, se for o caso.

As leis que norteiam o nosso procedimento de segurança da informação estão abaixo listadas:

- Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados;
- Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a Proteção da Propriedade Intelectual do Programa de Computador;
- Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;
- Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de Colaboradores que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;
- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse de segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;
- Lei nº 12.527, de 18 de novembro de 2011, regula o acesso a informações;
- Lei nº 12.965, de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Decreto nº 8.771, de 11 de maio de 2016, regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na

internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações;

- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD);
- NBR/ISO/IEC 17799, que institui o código de melhores práticas para gestão de segurança da informação;
- Consolidação das Leis Trabalhistas (CLT), Súmulas e Orientações Jurisprudenciais dos Tribunais Trabalhistas.

14. Informações e Dúvidas

Todas as informações necessárias sobre regras e princípios da JBJ Agropecuári estarão disponíveis nos Programas e Códigos adotados pela empresa,

disponíveis nos websites www.jbjagropecuaria.com.br e www jbjagropecuaria.com, bem como através de cópias impressas na empresa.

Em caso de dúvida sobre como proceder diante de determinada situação ou de como conduzir os negócios, o Comitê de Compliance/ Compliance Officer estará disponível para auxiliar todos da JBJ Agropecuária, bem como terceiros e parceiros.

Por fim, há a disponibilização do Canal de Ética para aqueles que quiserem auxílio de forma sigilosa, sem se identificar, o qual também estará disponível 24h por dia nos websites acima citados.

15. Definições

15.1 DEFINIÇÕES DA LEI GERAL DE PROTEÇÃO DE DADOS

- **Anonimização** – utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (art. 5º, inciso XI da Lei 13.709/2018 – LGPD). O dado anonimizado, nos termos da lei, deixa de ser considerado dado pessoal, garantindo maior liberdade no seu tratamento (art. 12 da Lei 13.709/2018 – LGPD);
- **Dado pessoal** – informação relacionada a pessoa natural

identificada ou identificável (art. 5º, inciso I da Lei 13.709/2018 – LGPD);

- **Dado pessoal sensível** – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, inciso II da Lei 13.709/2018 – LGPD);
- **Finalidade** – realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, inciso I da Lei 13.709/2018 – LGPD);
- **Necessidade** – limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (art. 6º, inciso III da Lei 13.709/2018 – LGPD);
- **Tratamento de Dados Pessoais** – toda operação realizada com dados pessoais, como as que se referem a: (art. 5º, inciso X da Lei 13.709/2018 – LGPD):
- **Acesso** - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição aplicável;
- **Armazenamento** - ação ou resultado de manter ou conservar um dado para consultas periódicas;
- **Arquivamento** - ato ou efeito de manter registrado um dado, embora já tenha perdido a validade ou esgotado a vigência para utilização;
- **Avaliação -** analisar o dado com o objetivo de produzir outras informações;
- **Classificação** - maneira de ordenar os dados conforme algum critério estabelecido e para alguma finalidade específica;
- **Coleta** - recolhimento de dados com finalidade específica;
- **Comunicação** - transmitir informações pertinentes aos dados para que seja traçado um plano de ação;
- **Controle** - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- **Difusão** - ato ou efeito de divulgação, propagação, multiplicação dos dados;
- **Distribuição** - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- **Eliminação** - ato ou efeito de excluir ou destruir o dado de onde ele está armazenado;

- **Extração -** ato de copiar ou retirar dados do armazenamento em que se encontrava;
- **Modificação** - ato ou efeito de alteração do dado;
- **Processamento** - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;
- **Produção** - criação de bens e de serviços a partir do tratamento de dados;
- **Recepção** - ato de receber os dados ao final da transmissão;
- **Reprodução** - cópia de dado preexistente obtido por meio de qualquer processo;
- **Transferência** - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- **Transmissão** - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, etc.;
- **Utilização** - ato ou efeito do aproveitamento dos dados.
- **LGPD (Lei Geral de Proteção de Dados)** – Lei 13.709/2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (art. 1º da Lei 13.709/2018 – LGPD).

15.2. DEFINIÇÕES DE SEGURANÇA DA INFORMAÇÃO

- **Ameaça** – causa potencial de violação da Segurança da Informação.
- **Departamento de Tecnologia da Informação** – departamento responsável pelo planejamento, coordenação, organização, manutenção, controle e supervisão dos recursos de tecnologia da informação.
- **Informação** – todo dado que de alguma forma possui significado e relevância para quem o recebe.
- **Material de consumo em informática** – trata-se de materiais utilizados, direta ou indiretamente, para armazenar, transmitir, e disseminar informações na área de informática, tais como: cartões de memória, pen drives.
- **Propriedade intelectual** – todas as informações desenvolvidas na prestação de serviços para a JBJ.
- **Recursos de Tecnologia da Informação** – equipamentos, instalações, softwares, sistemas, serviços, informações, redes e tecnologias, direta ou indiretamente administradas pelo departamento de tecnologia da informação e destinados a armazenar, processar, transmitir, e disseminar informações de interesse da JBJ, entre eles: computadores, computadores

portáteis e outros terminais; impressoras, scanners e periféricos; servidores de rede; modems, roteadores, comutadores e racks de equipamentos; componentes de cabeamento de rede; sistemas operacionais, aplicativos e quaisquer outros softwares; correio eletrônico; bancos de dados, documentos ou quaisquer outros tipos de informação armazenados, processados ou transmitidos em meio digital; contas de rede, contas de correio eletrônico, senhas e outros tipos de contas de acesso; enlaces de comunicação de dados; no-breaks e estabilizadores de tensão, quando sob a responsabilidade da Departamento de Tecnologia da Informação; sala de servidores;e manuais técnicos.

- **Segurança da Informação** – conjunto de medidas que visam a proteção das informações, assegurando-lhes confidencialidade, disponibilidade e integridade.
- **Usuário –** toda pessoa física ou jurídica com a devida autorização para utilizar recursos de Segurança da Informação e material de consumo em informática da empresa.

Data	Alterações Realizadas	Aprovada	Próxima Revisão
20/09/2021	ADEQUAÇÃO LGPD	FABRÍCIO BATISTA	09/2022

Declaro que recebi, li e concordo com a Política de Segurança da Informação da JBJ.

Estou ciente de que o não cumprimento desta Política é passível das penalidades previstas na mesma.

Matrícula: _____

Data: _____/_____/_____

Nome: _____

_____

Assinatura: _____

JBJ
AGROPECUÁRIA

JBJ
AGROPECUÁRIA