Título:	**Política Pública de Segurança da Informação**		
Área emitente:	**00.Políticas Corporativas**	**Data:**	**10/02/2023**
Código:	**PC.00.0070**	**Revisão:**	**1**

Sumário

Título:	**Política Pública de Segurança da Informação**		
Área emitente:	**00.Políticas Corporativas**	**Data:**	**10/02/2023**
Código:	**PC.00.0070**	**Revisão:**	**1**

1 – OBJETIVO

O objetivo deste documento é estabelecer diretrizes, quanto ao gerenciamento e controles de segurança da informação e segurança cibernética na Suzano, buscando mitigar vulnerabilidades, preservar e proteger os ativos, principalmente a informação e os dados pessoais, conforme leis, regulamentações e obrigações contratuais vigentes, contemplando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação.

O controle estratégico de riscos e de segurança da informação é de responsabilidade da área de **Segurança da Informação** e deve ser observado por todos os usuários da Suzano que tratam a informação em todo seu ciclo de vida.

1.1 - Abrangência

Este documento se destina a todos os usuários, que tratam ou possam tratar informações, incluindo dado pessoal em ativos locais ou em nuvem, alocados dentro ou fora da Suzano, geridos pela Suzano e/ou por Empresa Prestadora de Serviços.

2 – DOCUMENTOS DE REFERÊNCIA

- Código de Conduta da Suzano;
- ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos;
- ABNT NBR ISO/IEC 27002:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.

3 – TERMOS, DEFINIÇÕES E ABREVIATURAS

- **Ameaça:** Potencial causa de um incidente de segurança indesejado que pode resultar em dano a um sistema ou organização;
- **Ativo:** Tudo que tenha valor para a organização, material ou não;
- **Autenticidade:** Propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
- **Canal Peipedê:** Central de Privacidade e Proteção de Dados Pessoais da Suzano para atendimento quanto às solicitações relacionadas ao exercício dos direitos dos titulares recebidas pela organização (Website: https://ppd.suzano.com.br).
- **Colaborador:** Categoria que engloba todos os empregados, estagiários, aprendizes que prestam serviços e de qualquer forma estejam alocados e possuam vínculo empregatício com a Suzano;
- **Confidencialidade:** Garantia de que a informação é acessível somente por pessoas autorizadas;
- **Dados Pessoais:** Toda e qualquer informação relacionada à pessoa natural (física) identificada ou identificável, incluindo dados pessoais sensíveis (origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico, ou político ou

moral, dado referente à saúde ou à vida sexual, dado genético ou biométrico). A depender da jurisdição de privacidade e proteção de dados aplicável, podem ser considerados dados pessoais sensíveis informações pessoais que revelam: previdência social, carteira de motorista, carteira de identidade estadual ou número do passaporte de um consumidor; login da conta de um consumidor, conta financeira, cartão de débito ou número de cartão de crédito em combinação com qualquer código de segurança ou acesso, senha ou credenciais que permitam o acesso a uma conta; geolocalização precisa do consumidor e; conteúdo do correio, e-mail e mensagens de texto de um consumidor, a menos que a empresa seja a destinatária da comunicação. O conceito de dados pessoais não se limita a informações que possam ser consideradas prejudiciais à vida privada e familiar do indivíduo. Nem o meio em que a informação está contida é relevante: o conceito de dados pessoais inclui informações disponíveis sob qualquer forma: texto, figuras, gráficos, fotografia, vídeo, acústico ou qualquer outro meio possível que leve a identificação do sujeito de modo direto ou indireto.

- **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **DPO (Data Protection Officer) | DPO Funcional ou Encarregada de Dados**: Pessoa que supervisiona e oferece suporte em todos os temas relacionados ao tratamento de dados pessoais, de acordo com o que está previsto nas legislações de proteção de dados pessoais locais e estrangeiras aplicáveis, bem como disposto em políticas e procedimentos internos da Suzano sobre privacidade e proteção de dados pessoais, além de ser o canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
- **Empresa Prestadora de Serviços (EPS):** Empresa prestadora de serviços ou empresa fornecedora de bens com serviços atrelados;
- **Incidente de Segurança:** Qualquer evento adverso, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a confidencialidade, a integridade, disponibilidade, a autenticidade e a legalidade de qualquer ativo de informação da Companhia;
- **Incidente de Privacidade e Proteção de Dados Pessoais:** Um incidente de privacidade e proteção de dados pessoais ("Incidente P&PD") é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados pessoais inadequados ou ilícitos, os quais possam ocasionar riscos para os direitos e liberdades do titular dos dados pessoais.
- **Informação:** Dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- **Integridade:** Salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- **Least Privilege**: Princípio do menor privilégio, também conhecido como princípio do mínimo privilégio ou princípio da menor autoridade, exigido para desempenho da atividade executada;
- **Legalidade:** Ou não repúdio, uso da tecnologia de informática e comunicação deve estar de acordo com as leis vigentes no local ou país;
- **Need To Know:** Princípio do acesso apenas aos dados que são necessários para o desempenho da função;

- **Política Corporativa (PC):** Expressa o direcionamento estratégico da Suzano S.A. e permeia toda Companhia;
- **Recursos Móveis:** Quaisquer equipamentos eletrônicos com atribuições de mobilidade fora do perímetro físico da Suzano;
- **Suzano ou Companhia:** Suzano S.A., suas subsidiárias e suas controladas (em conjunto "Suzano" ou "Companhia"), controlada (ou controle) sendo considerada a sociedade na qual a controladora, diretamente ou através de outras controladas, é titular de direitos de sócio que lhe assegurem, de modo permanente, preponderância nas deliberações sociais e o poder de eleger a maioria dos administradores. Para os fins dessa Política, considera-se "controladas" as entidades nas quais a Companhia possua participação direta ou indireta superior ao equivalente à 50% (cinquenta por cento) do capital social;
- **Titular dos dados:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (por exemplo: colaborador, ex-colaborador, candidato à entrevista, consumidor final, terceiros etc.).
- **Trabalho Remoto (Home Office):** Refere-se aos ambientes de trabalhos não tradicionais, quer dizer todas as formas de trabalho fora do escritório, tais como: teletrabalho, trabalho virtual, trabalho flexível, trabalho híbrido etc.;
- **Tratamento de dados pessoais:** Toda operação realizada com dados pessoais, tais como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Usuário:** Engloba todo colaborador da Suzano e Empresa Prestadora de Serviços que possui vínculo empregatício e/ou contratual que no âmbito desta relação, trata ou possa tratar informação, incluindo dado pessoal.
- **Vulnerabilidade:** Fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

4 – DIRETRIZES

4.1 - Diretrizes Gerais

As diretrizes relativas à área da **Segurança da Informação**, mencionadas a seguir, devem ser cumpridas por todos os usuários da Suzano. As informações e dados pessoais devem ser utilizadas exclusivamente para o interesse da Companhia e cada usuário deve ter seu acesso restrito às informações e aos recursos a que esteja devidamente autorizado.

A implementação de controles de segurança da informação, tanto na atuação no ambiente local da Suzano, quanto no trabalho remoto (Home Office) deve ser observado e garantido o nível adequado de segurança, para a prevenção e proteção dos ativos em todo seu ciclo de vida.

4.2 - Controle de Acesso Lógico

O acesso às informações deve ser controlado e disponibilizado conforme as atribuições de cada usuário, ou seja, aplicando os princípios “Need To Know” e “Least Privilege”. As contas de acesso lógico são intransferíveis, sendo de responsabilidade de seu titular quaisquer acessos realizados.

4.3 - Controle de Acesso Físico

É imprescindível um nível de segurança física adequado, para prevenção e proteção do acesso às dependências da Suzano para inibição de acesso não autorizado, evitando danos ao patrimônio, ao negócio, às pessoas e à informação. É importante também que às dependências sejam protegidas, minimizando possíveis riscos, decorrentes de ameaças externas, tais como: desastres naturais, ataques maliciosos, acidentes, entre outros.

4.4 - Classificação da Informação

A informação deve ser classificada pelo proprietário da informação, em termos do seu valor para o negócio, sensibilidade e criticidade, inclusive atendendo requisitos legais, regulatórios e obrigações contratuais vigentes, para evitar a modificação e/ou divulgação não autorizada. O proprietário da informação deve considerar o nível de confidencialidade, integridade, disponibilidade, autenticidade e legalidade, atentando-se para as mudanças de sua criticidade ao longo do tempo e às necessidades do negócio.

4.5 - Gestão de Ativos

A existência de um inventário único e constantemente atualizado é primordial para o negócio e contribui para a efetiva proteção dos ativos. Portanto, todos os ativos da Suzano devem ser identificados com um nível de detalhe adequado e possuir um proprietário atribuído. Além disso, deve ser garantido a classificação, o monitoramento e a gestão dos dados associados em todo seu ciclo de vida.

4.6 - Uso Aceitável dos Ativos

Qualquer informação acessada, transmitida, recebida ou produzida utilizando-se dos ativos de propriedade da Suzano devem ser utilizados apenas para fins profissionais, de modo lícito, ético e moral.

4.6.1 - Recurso Móvel e Trabalho Remoto

Para que a informação pertinente ao negócio não seja comprometida, deve ser assegurado controles de segurança da informação aos recursos móveis e tecnológicos, levando em consideração a possibilidade do trabalho em ambientes desprotegidos ou em ambientes de trabalho remoto (Home Office).

Deve ser estabelecido o monitoramento e a proteção para mitigar vulnerabilidade, evitando: o vazamento, destruição, perda ou roubo, alteração ou acesso não autorizado ao dado pessoal, informação confidencial ou restrita.

4.6.2 - Restrição de Instalação de Software

Não é permitido a utilização de Software não homologado pela Suzano. Portando é vedado qualquer tipo de instalação não autorizada de qualquer tipo de Software não licenciado na Companhia.

4.6.3 - Propriedade Intelectual

Tecnologias, obras intelectuais, Softwares, desenhos industriais, marcas, identidade visual, sinal distintivo, metodologias e quaisquer informações atuais ou futuras que pertençam à Suzano, em qualquer suporte, inclusive na internet e mídias sociais, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio usuário em seu ambiente de trabalho.

4.7 - Backup e Restore

Deve ser mantido um processo de armazenamento de cópia de segurança dos ativos e recuperação da informação, com o propósito de garantir a disponibilidade da informação, quando necessário ou na ocorrência de algum evento que possa causar algum tipo de impacto na Companhia.

As cópias de segurança e recuperação devem ser devidamente testadas periodicamente, em intervalos previamente definidos, para que seja identificado uma recuperação satisfatória dos ambientes de produção ou em caso de incidente de segurança da informação, garantir a continuidade do negócio.

4.8 - Proteção Contra Malware

Deve ser implementado e mantido atualizado, solução de segurança que permita a detecção, prevenção, recuperação e erradicação de todas as classes de Softwares maliciosos, para proteção contra Malware. Deve ser garantido a atualização constante de uma lista de liberação de bloqueio de Websites maliciosos ou usar uma lista pública para esta finalidade.

4.9 - Gestão de Vulnerabilidades

Deve ser garantido o gerenciamento de vulnerabilidades nos ativos locais ou na nuvem, alocados dentro ou fora da Suzano, através de ações de prevenção para atender a necessidade do negócio. É preciso reduzir os riscos de exposição cibernética, através da identificação, classificação e mitigação de vulnerabilidades, evitando impactos provenientes de exploração de ameaças internas e/ou externas, nos ambientes da Companhia.

4.10 - Gestão de Incidente de Segurança da Informação

A detecção rápida de um incidente de segurança da informação, contribui para redução de possível perda financeira, danos à imagem e reputação, exposição de dado pessoal, paralisação da operação, entre outros, além da recuperação controlada de um incidente de segurança.

Portanto, todo risco ou possível incidente de segurança da informação deve ser comunicado imediatamente, através dos canais de comunicação internos da Suzano ou externo através do e-mail CSIRT@suzano.com.br.

Em caso de incidente de privacidade e proteção de dados pessoais ("Incidente P&PD") deve ser reportado imediatamente através do Canal Peipedê, que se encontra disponível do Website https://ppd.suzano.com.br ou através do e-mail LGPD@suzano.com.br.

4.11 - Gestão de Riscos

Deve ser definida e implementada uma metodologia de identificação, análise, monitoramento e comunicação de riscos de segurança da informação, de forma gerenciada, garantindo a devida resposta a qualquer risco que possa impactar a Suzano. O processo deve ser realizado, de forma contínua e, de acordo com a necessidade da Companhia, com o propósito de promover as medidas de segurança da informação mais adequadas e, assim, reduzir a exposição a ameaças e a probabilidade de causar algum tipo de dano a qualquer ativo tangível ou intangível da Suzano.

4.12 - Hardening e Patch

A gestão de Hardening deve ser definido e implementado, para redução de riscos de exposição dos ativos, através da eliminação ou limitação dos vetores de ataques em potencial ou diminuição da superfície de ataque. O intuito é remover configurações supérfluas, funções padrões em contas, Software, portas, permissões, acessos, etc. desnecessários.

A gestão de Patch deve ser definida e implementada, para distribuição, teste e aplicação segura do Software, ou seja, a atualização de segurança permite a correção de vulnerabilidade, que são suscetíveis a ataques cibernéticos, além de garantir o suporte adequado, a conformidade com as legislações, regulamentações e obrigações contratuais vigentes e proporcionando as melhorias de recursos inerentes ao Software.

4.13 - Rastreabilidade

Os registros de eventos de acesso aos ativos, considerados críticos e que trafegam informação classificada como confidencial e restrita devem ser coletados automaticamente, de forma estruturada, ser adequadamente protegidos, para que seja evitado modificações não autorizadas, garantindo a integridade e autenticidade, inclusive devem ser monitorados e armazenados por período razoável, para estar disponível, quando solicitado.

4.14 - Segurança Cibernética

Deve ser garantida a segurança cibernética, para promoção de ações voltadas para a segurança de operações, através de mitigação de vulnerabilidades, de forma a garantir que os ativos sejam capazes de resistir a eventos no espaço cibernético, com a possibilidade de comprometimento da disponibilidade, integridade, confidencialidade, autenticidade e legalidade dos dados armazenados, processados ou transmitidos.

4.15 - Segurança Industrial

Deve ser garantindo a segurança da informação e cibernética no setor industrial, pois a convergência entre as plantas industriais e a área de Tecnologia da Informação está aumentando, intensificando cada vez

mais a conectividade, promovendo aumento na automação, na comunicação e no monitoramento, havendo maior eficiência.

4.16 - Segurança na Empresa Prestadora de Serviço

Devem ser definidos critérios mínimos de segurança da informação, de forma a mitigar os riscos e proteger os ativos da Suzano que são acessíveis pela Empresa Prestadora de Serviços (EPS). O prestador de serviços é responsável pela guarda segura e sigilosa da informação, conforme cláusula de confidencialidade, firmado em contrato e legislação vigente.

4.17 - Conscientização e Treinamento

A área de **Segurança da Informação** deve definir um processo que implemente, monitore e mensure ações estruturadas, que indique, promova e supra atividades relativas à conscientização e treinamento em segurança da informação e segurança cibernética, de forma regular. O intuito é disseminar o conhecimento e qualificar os usuários para prevenção e proteção dos ativos da Suzano, contra ameaças.

4.18 - Gestão de Continuidade de Negócios (Resiliência)

Deve ser garantido que os recursos mínimos (pessoas, processos e tecnologia), sejam preservados em um momento de ruptura, permitindo uma redução de impacto e retomada das atividades críticas da Suzano. Desta forma, é necessária a definição de uma metodologia para acompanhamento das principais iniciativas sobre continuidade de negócio, recuperação de desastres e gestão de crises, através da identificação e priorização das funções e processos críticos que podem causar maior impacto caso não estejam disponíveis.

4.19 - Privacidade e Proteção de Dados Pessoais

Todos são responsáveis por assegurar a proteção dos dados pessoais que se tem acesso, incluindo, mas não se limitando a proteção de acesso indevido ou não autorizado. As medidas de segurança necessárias para garantir a segurança dos dados pessoais devem ser aplicadas, buscando a preservação da informação, inclusive dados pessoais de terceiros que eventualmente se teve acesso durante ou após o vínculo estabelecido entre a Empresa Prestadora de Serviços, Terceiros e a Suzano.

Não é permitido copiar e/ou compartilhar quaisquer documentos, planilhas, contratos ou contatos dos clientes, Empresas Prestadoras de Serviços (EPS), colaboradores(as) e parceiros(as) de negócio da Suzano que contenham dado pessoal fora do contexto específico do trabalho e das políticas internas, sob pena de ferir o Código de Conduta e as legislações de proteção de dados pessoais vigentes.

A Suzano tem um compromisso com o tratamento legítimo e lícito dos dados pessoais de todas as pessoas naturais (físicas), ou seja, os titulares de dados pessoais que interagem conosco: colaboradores(as), acionistas, clientes e representantes dos parceiros(as) de negócios.

A privacidade e a proteção de dados pessoais são direitos fundamentais e, a Suzano, possui o compromisso de resguardar esses direitos e para isso, segue os seguintes princípios: não discriminação, transparência, segurança, qualidade dos dados, minimização, livre acesso, prevenção, responsabilização e prestação de contas. Toda e qualquer atividade de tratamento de dados pessoais deve sempre respeitar e

assegurar conformidade com as leis e os regulamentos aplicáveis, agindo sempre com transparência e respeitando a finalidade para qual os dados pessoais foram coletados.

A privacidade e a proteção dos dados pessoais devem ser consideradas durante todo o ciclo de vida dos dados pessoais, desde a coleta, descarte, armazenamento, compartilhamento e uso lícito dos dados pessoais.

Para mais informações sobre como o dado pessoal é tratado, acesse o Canal Peipedê que se encontra disponível no Website https://ppd.suzano.com.br.

4.20 - Histórico de Revisão

Nº Versão	Descrição	Data
0	Emissão Inicial	19/04/2022
1	Inclusão de novas definições no item 3 – Termos, Definições e Abreviaturas; Inclusão do item 4.2 – Controle de Acesso Físico; Alteração do e-mail de reporte a incidente de segurança da informação, de: ciberseguraca@suzano.com.br, para: CSIRT@suzano.com.br; Inclusão do Canal Peipedê; Atualização do item 5 – Responsabilidades.	Documento Vigente

5 – RESPONSABILIDADES

Matriz RACI				
Descrição das Principais Atividades	**Usuário**	**Proprietário da Informação**	**Segurança da Informação**	**P&PD**
1 - Objetivo				
Aplicar controle estratégico de riscos e de segurança da informação;	I		A/R	
4.1 - Diretrizes Gerais				
Cumprir todas as diretrizes de segurança da informação;	A/R			
4.2 - Gestão de Acesso Lógico				
Realizar proteção, sigilo e utilização de credenciais e senhas;	A/R			
4.4 - Classificação da Informação				
Classificar e tratar a informação, em termos do seu valor para o negócio, sensibilidade e criticidade, inclusive atendendo requisitos		A/R		

Matriz RACI				
Descrição das Principais Atividades	**Usuário**	**Proprietário da Informação**	**Segurança da Informação**	**P&PD**
legais, regulatórios e contratuais;				
4.7 - Backup e Restore				
Manter um processo de armazenamento de cópia de segurança dos Ativos TIC e recuperação da informação e/ou dados;		A/R		
4.8 - Proteção Contra Malware				
Implementar e manter atualizado, solução de segurança que permita a detecção, prevenção, recuperação e erradicação de todas as classes de Softwares maliciosos;			A/R	
4.9 - Gestão de Vulnerabilidades				
Garantir o gerenciamento de vulnerabilidades nos Ativos TIC local ou na nuvem, alocados dentro ou fora da Suzano			A/R	
4.10 - Gestão de Incidente de Segurança da Informação				
Notificar todo risco ou possível incidente de segurança da informação, sem demora, através dos canais de comunicação da Suzano;	A/R		I/C	
4.16 - Segurança na Empresa Prestadora de Serviços				
Definir critérios mínimos de segurança da informação, de forma a mitigar os riscos e proteger os ativos da Suzano que são acessíveis pela Empresa Prestadora de Serviços (EPS);			A/R	
4.17 - Conscientização e Treinamento				
Definir um processo que implemente, monitore e mensure ações estruturadas, que indique, promova e supra atividades relativas à conscientização e treinamento em segurança da informação e segurança cibernética;			A/R	
4.18 - Gestão de Continuidade do Negócio (Resiliência)				
Garantir que os recursos mínimos (pessoas, processos e tecnologia), sejam preservados em um momento de ruptura, permitindo uma redução de impacto e retomada das atividades críticas da Suzano;			A/R	
4.19 - Privacidade e Proteção de Dados Pessoais				
Compartilhar de quaisquer documentos, planilhas, contratos ou contatos dos clientes, Empresas Prestadoras de Serviços (EPS),	A/R		C	C

Matriz RACI				
Descrição das Principais Atividades	**Usuário**	**Proprietário da Informação**	**Segurança da Informação**	**P&PD**
colaboradores(as) e parceiros(as) de negócio da Suzano que contenham dados pessoais fora do contexto específico do trabalho e das políticas internas NÃO é permitido.				
Considerar a privacidade e a proteção de dados pessoais durante todo o ciclo de vida dos dados pessoais, desde a coleta, descarte, armazenamento, compartilhamento e uso lícito dos dados pessoais.	A/R		C	C
Resguardar os direitos de privacidade e a proteção de dados pessoais, são direitos fundamentais e, a Suzano, segue os seguintes princípios: não discriminação, transparência, segurança, qualidade e minimização.	R			A/R
Tratar e usar os dados pessoais respeitando sempre as leis e os regulamentos aplicáveis, agindo sempre com transparência e à finalidade para que é utilizado os dados pessoais.	A/R			C

Legenda: **A** - Autoridade | **C** - Consultado | **I** - Informado | **R** – Responsável

6 – APROVAÇÃO DA POLÍTICA

A presente Política entra em vigor, na data de sua aprovação mínima do Gerente Executivo de Tecnologia da Informação que é o órgão da Companhia que possui competência exclusiva para alteração, em qualquer hipótese, desta Política.

Nota1: se necessário, cópias da deliberação sobre a alteração ou revisão da Política podem ser enviadas para partes interessadas.

7 – VIOLAÇÃO DA POLÍTICA

As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas da Suzano, na legislação vigente no Brasil e nos países onde as empresas estão localizadas.

8 – CONSIDERAÇÕES FINAIS

Esta política deve ser pública. É de responsabilidade de todos os usuários o acompanhamento da atualização desta política, sendo vedado alegar seu desconhecimento.

9 – ANEXOS

Não Aplicável.