ANEXO DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Este documento tem como objetivo a formalização dos requisitos mínimos de segurança da informação, tanto lógica, quanto física, visando a proteção das informações da Suzano, principalmente dados restritos e confidenciais, alocados dentro ou fora do ambiente da Suzano, em contratos com as Empresas Prestadoras de Serviços (EPS). Este documento se aplica a qualquer Empresa Prestadora de Serviços que trata ou venha a tratar (acessar, modificar, armazenar, transmitir etc.) informações da Suzano, seja no ambiente Corporativo ou Industrial.

Todos os documentos normativos publicados e sob a responsabilidade da Suzano, inclusive a **Política Pública de Segurança da Informação**, disponibilizada no Website da Suzano, cujo conteúdo está disponível em **Documentos e Políticas** , devem ser seguidos pelas Empresas Prestadoras de Serviços que possuam contrato, que no âmbito desta relação, tratam ou possam tratar informações.

A Suzano se reserva ao direito de realizar testes, solicitar correções e evidências sempre que entender que seja necessário, conforme criticidade e necessidade.

Importante:

- A Empresa Prestadora de Serviços deve atender, mas não se limitar os seguintes requisitos mínimos de segurança da informação descritos abaixo, levando em consideração os requisitos mínimos de segurança da informação que se aplicam tanto ao ambiente Corporativo, quanto ao ambiente Industrial;
- É imprescindível que Empresa Prestadora de Serviços verifique a aplicabilidade de cada um dos requisitos mínimos de segurança da informação, levando em consideração o contexto da contratação. Portanto, tópicos listados nesse Anexo de Segurança da Informação que não são aplicáveis podem ser ignorados;
- Todas as recomendações das melhores práticas nacionais e internacionais, principalmente: NIST Cybersecurity Framework, NIST 800-82 guia “Cybersecurity for Industrial Control Systems”, ISA/IEC 62443 e ISO/IEC 27001 devem ser atendidas.

2. GLOSSÁRIO

- **Ativo TIC (Tecnologia de Informação e Comunicação):** Toda tecnologia que permite o acesso, armazenamento, transmissão, arquivamento e manipulação da informação, tais como, porém, não se limitando a: aplicativos, sistemas, ferramentas de desenvolvimento, utilitários, ativos de automação Industrial, ativos virtuais, ativos de rede, entre outras ferramentas que venham ser utilizadas no futuro, devido a inovação tecnológica;
- **EPS:** Empresa Prestadora de Serviços ou empresa fornecedora de bens com serviços atrelados;
- **Informação Confidencial:** Pode ser atribuída a qualquer informação considerada altamente estratégica e crítica, por exemplo: segredos industriais, propriedade intelectual, estratégia de Marketing e vendas, dados financeiros, credenciais e senhas etc., incluindo os dados pessoais de usuários, clientes, partes externas, dentre outros;
- **Suzano ou Companhia:** Suzano S.A., suas subsidiárias e suas controladas;
- **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.

3. DIRETRIZES DO PROCESSO

3.1. Análise de Vulnerabilidade e Pentest

É imprescindível que a Empresa Prestadora de Serviços realize testes de segurança da informação periodicamente, para sanar previamente as vulnerabilidades existentes, com o objetivo de manter seu ambiente atualizado e seguro, seguindo as melhores práticas internacionais e a notificação de vulnerabilidades críticas e planos de ação para correção. Deve também, quando solicitado pela Suzano, fornecer os resultados dos testes realizados.

A Suzano se reserva ao direito de realizar testes de vulnerabilidades e Pentest (teste de invasão), quando aplicável e acordado com a Empresa Prestadora de Serviços, conforme criticidade e necessidade. Para fins de validação por parte da Suzano, um teste de vulnerabilidade pode ser realizado para comprovação de correções. Os testes são repetidos até que as falhas identificadas sejam corrigidas e aprovadas pela área de **Cibersegurança** da Suzano.

No entanto, caso sejam identificadas falhas durante a análise de vulnerabilidade pela Suzano, ou até mesmo identificado por qualquer meio, seja por mídias, fóruns de segurança, Bug Bounty etc., na plataforma desenvolvida ou disponibilizada pela Empresa Prestadora de Serviços, esta, após a notificação formalizada pela Suzano, deve saná-las imediatamente e tempestivamente, conforme periodicidade pré-determinada pela Suzano.

Caso a Empresa Prestadora de Serviços comprove tecnicamente a não aplicabilidade da correção, esta será responsável pelos eventuais danos gerados à Suzano e suas partes relacionadas em razão das vulnerabilidades detectadas e notificadas.

Caso seja identificada a necessidade de qualquer ação de correção de fragilidades de segurança da informação no ambiente, que seja de responsabilidade da Suzano, a área de **Cibersegurança** deve ser informado de maneira explícita e específica no prazo de 48 (quarenta e oito) horas, através do e-mail CSIRT@suzano.com.br.

Importante: A não realização da análise de vulnerabilidade em Ativos TIC ou a não comprovação das correções sugeridas pela Suzano pode ser considerado como um descumprimento de contrato ou omissão por parte da Empresa Prestadora de Serviços.

3.2. Auditoria

A Suzano se reserva ao direito de realizar auditorias, previamente alinhadas com a EPS, para verificar a efetividade dos controles de segurança da informação implementados. No caso de uma avaliação de maturidade de segurança da informação da Empresa Prestadora de Serviços, esta deve responder ao questionário de avaliação e enviar as evidências comprobatórias, de forma que

se mantenha a confidencialidade de suas informações, no que tange a controles e políticas de segurança da informação implementadas, quando solicitadas pela Suzano.

3.3. Conscientização e Treinamento

A Empresa Prestadora de Serviços deve disponibilizar periodicamente aos seus colaboradores: treinamento, educação e conscientização em segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, políticas e procedimentos específicas por tema, pertinentes para as suas funções.

3.4. Continuidade dos Negócios

A Empresa Prestadora de Serviços deve manter atualizados e testados periodicamente um Plano de Continuidade de Negócios (PCN), além de apresentar planos de recuperação garantindo assim a continuidade dos negócios prestados à Suzano, para o caso, mas não se limitando a, de ocorrência de um incidente de segurança da informação, inclusive ataque cibernético, como por exemplo, Ransomware, que proporcione a interrupção de um serviço. A Empresa Prestadora de serviços deve prever, no mínimo, os casos de indisponibilidade de Ativo TIC, indisponibilidade de dependências ou indisponibilidade de usuários.

3.5. Desenvolvimento Seguro de Software

Para contratações envolvendo desenvolvimento de Softwares, aplicativos etc., a Empresa Prestadora de Serviços deve:

- Garantir e evidenciar a ausência de vulnerabilidades no código-fonte, para todos os módulos de Software que compõe o Ativo TIC, mesmo aqueles não desenvolvidos diretamente e, qualquer caso, seguir os padrões internacionais OWASP, SANS Institute etc.;
- Garantir um processo de desenvolvimento seguro de Software para mitigação dos riscos e vulnerabilidades catalogadas ou não, em tempo de desenvolvimento. Em caso de desenvolvimento ou customização para a Suzano, devem ser seguidos os processos e padrões já praticados pela Suzano, além de submeter o código a verificações de vulnerabilidades;
- Assegurar criação de perfis e usuários corporativos com o devido controle de acesso, garantindo o Need to Know e o Least Privilege;
- Assegurar sanitização de toda informação que se encontre em ambiente de homologação ou teste;
- Garantir que não são utilizados dados reais nos ambientes de homologação ou teste. Deve ser gerada uma base sem informações verdadeiras ou mascaradas para utilização durante os testes;
- Caso trafeguem dados de cartão de crédito, o Software deve ser desenvolvido, de acordo com o padrão PCI-DSS.

3.6. E-mail Corporativo Suzano S.A.

Caso o prestador de serviços, vinculado a Empresa Prestadora de Serviços, receba o e-mail corporativo da Suzano, deve-se haver a preocupação em utilizar exclusivamente para o desempenho das atividades laborais firmadas em contrato, observando as obrigações legais e regulamentares vigentes. Deve ser observado:

- A conta do e-mail não deve ser compartilhada com outros usuários;
- A informação deve ser classificada, antes do envio do e-mail e destacada de acordo com a sua sensibilidade, principalmente informação confidencial, conforme **Política Pública de Segurança da Informação**;
- Anexos de origem desconhecida não devem ser abertos e links suspeitos não devem ser clicados;
- Não utilizar o e-mail para cadastros em sites externos;
- Em caso de qualquer tipo de suspeita de um incidente de segurança da informação, notificar imediatamente através do e-mail CSIRT@suzano.com.br.

3.7. Estações de Trabalho, Servidores e Demais Dispositivos

Considerando as estações de trabalho, servidores e demais dispositivos utilizados e pertencentes a Empresa Prestadora de Serviços, incluindo qualquer mídia removível, utilizada para desempenho das atividades de trabalho prevista em contrato com a Suzano, deve ser garantido:

- Realizar por meio de credenciais de acesso individual, assegurando um ID único e uma autenticação através de senha forte, utilizando o duplo fator de autenticação, para os acessos realizados;
- Manter um processo de atualização de Software dos Ativos TIC necessários para corrigir falhas ou defeitos, evitando possíveis vulnerabilidades;
- Possuir uma rotina de atualização de antivírus e com a função “monitoramento” sempre ativo. Além disso, desabilitar a opção “desativar antivírus” para o usuário final. Na ocorrência de algum incidente de segurança da informação com a identificação de vírus, a área de **Cibersegurança** da Suzano, por meio do e-mail CSIRT@suzano.com.br, deve ser notificada, em até 24 (vinte quatro) horas;
- Os dados não devem ser armazenados, exceto nos casos em que é previsto em contrato, para atendimento das finalidades do serviço ou atividade contratada, devendo a Empresa Prestadora de Serviços ser responsável por aplicar as medidas de segurança necessárias para proteção da informação, bem como realizar os devidos descartes, a fim de evitar todo e qualquer acesso não autorizado e/ou uso indevido em caso de Job Rotation ou Turn Over;
- Garantir o bloqueio de tela através de senha e por tempo de inatividade nas estações de trabalho;
- As estações de trabalho da Empresa Prestadora de Serviços, quando conectadas à rede da Suzano, devem:
    - Bloquear Portas periféricas (USB, USB-C e SD) evitando uso de dispositivos removíveis;
    - Estar equipadas com Firewall, sendo desejável também Host IPS ou EDR/XDR;

- Estar livres de Software que contenham ferramentas capazes de permitir que sistemas certificados na Internet interajam, acessem ou gerenciem os Ativos TIC, por meio de fluxos de comunicação encapsulados no tráfego transmitido por Proxy;
- Não devem ser utilizados como dispositivos pontes, para interconexão de redes lógica ou fisicamente segregados, em particular estações de trabalho equipados com mais de uma interface de conexão;
- Ter acesso à Internet restrito e controlado por Proxy com políticas de proteção a site malicioso, com a finalidade de proteger qualquer tipo de acesso não autorizado;
- Manter os Patches atualizados.

3.8. Eventos e Incidentes de Segurança da Informação

- Deve-se garantir a segurança da informação do serviço prestado, identificando e fornecendo informações sobre o responsável, área e estrutura, no que tange os aspectos de segurança da informação, para assegurar as relações entre a Empresa Prestadora de Serviços e a Suzano, comunicando previamente qualquer alteração;
- A área de **Cibersegurança** deve ser notificada, quando na identificação ou suspeita de qualquer evento ou incidente de segurança da informação, sem discriminação, inclusive as acidentais, através do e-mail: CSIRT@suzano.com.br. A comunicação deve ser realizada em até 24 (vinte e quatro) horas, contanto a partir do conhecimento do evento ou do incidente de segurança da informação, compartilhando informações detalhadas, as vulnerabilidades encontradas e ações tomadas para mitigar a ação. Deve também, quando solicitado pela Suzano, fornecer informações inerentes ao evento ou incidente de segurança da informação;
- Todas as atividades inerentes a gestão de respostas a incidentes de segurança da informação devem ser documentadas e armazenadas, provendo toda a linha do tempo do processo de tratamento;
- A Empresa Prestadora de Serviços deve garantir a segurança necessária para casos de perda, furto ou roubo de equipamentos que possam conter informações de propriedade da Suzano, por meio de tecnologia de criptografia e assegurar a exclusão das informações. A Suzano deve ser notificada, conforme nota supracitada;
- A Empresa Prestadora de Serviços deve fornecer um canal de comunicação para que a área de **Cibersegurança** da Suzano se comunique, quando necessário, em caso de incidentes de segurança da informação;
- A Empresa Prestadora de Serviços deve se comprometer a colaborar com todas as ações necessárias para a tratativa de um incidente de segurança da informação que ocorrer em alguma das unidades da Suzano envolvendo Ativos TIC sob gestão da Empresa Prestadora de Serviços, em tempo hábil.

3.9. Proteção da Informação

A informação pode ser considerada o conjunto de dados estruturados e não estruturados, que podem estar relacionados a qualquer notícia ou comunicação verbal ou escrita, manual ou automática. No que diz respeito a Suzano, a informação expressa a ordenação e a organização dos dados que pode gerar valor e ter um significado para a Suzano, não importando a forma ou a tecnologia empregada, seja para o seu processamento, manipulação, transmissão, armazenamento etc. A partir desse conceito, a Empresa Prestadora de Serviços deve:

- Fornecer toda a informação documentada necessária para o desenvolvimento dos negócios em português (língua nativa do Brasil);
- Garantir que as informações sob a propriedade da Suzano sejam tratadas, de acordo com os princípios Need to Know e Least Privilege, além de aplicar a segregação de funções (SoD), exclusivamente dentro do serviço contratual, evitando a divulgação para usuários não autorizados;
- Salvaguardar a confidencialidade, integridade, disponibilidade, autenticidade e a legalidade, inclusive mantendo a conformidade com as legislações e regulamentações vigentes, de toda informação tratada na Suzano, independente do seu formato;
- Ter a completa rastreabilidade dos acessos realizados às informações da Suzano, com o intuito de identificar a origem, o autor, data e hora, além das informações acessadas, com o tempo mínimo de retenção de 12 (doze) meses;

Criptografar os dados confidenciais sob responsabilidade da Suzano em repouso e em trânsito, utilizando métodos fortes de criptografia, quando na manipulação, armazenamento ou transmissão. A Empresa Prestadora de Serviços deve assegurar que a Quarteirizada siga todos os requisitos mínimos de segurança da informação expressos neste documento. A Empresa Prestadora de Serviços é responsável por quaisquer contratações ou parcerias envolvidas na prestação do serviço a Suzano.

3.10. Soluções e Serviços em Nuvem

Para a Empresa Prestadora de Serviços que seja um provedor de serviços em nuvem ou que utilize os serviços deste para armazenamento de informação, deve-se garantir um ambiente de computação em nuvem seguro a Suzano, seguindo os requisitos do CSA (Cloud Security Alliance).

Para a Empresa Prestadora de Serviços que seja fornecedora de solução SaaS, deve-se garantir, além dos requisitos mínimos supracitados neste documento, mas não se limitando a:

- Deve haver segregação de funções nas atividades administrativas na console de gerenciamento da nuvem;
- Toda atividade de autenticação de usuários na console de gerenciamento da nuvem deve ser registrada em Log;
- Todos os acessos na console de gerenciamento da nuvem devem ser realizados através de métodos de autenticação forte, envolvendo pelo menos dois fatores de autenticação;
- As chaves criptográficas utilizadas na infraestrutura em nuvem não devem ser armazenadas ou transmitidas de forma clara;

- A solução em nuvem contratada pela Suzano deve possuir habilitado o gerenciamento de Logs centralizado, contendo os Logs de auditoria dos recursos em nuvem;
- Os Logs de auditoria dos recursos em nuvem contratados pela Suzano devem sempre estar disponíveis para acesso, em caso de suspeita de incidente de segurança da informação identificado pela Suzano;
- Deve estar habilitado o monitoramento na nuvem dos eventos para detecção de possíveis ataques cibernéticos e geração de alertas;
- Quando identificados incidentes ou eventos de segurança da informação, a solução em nuvem deve garantir a notificação de alertas;
- Os serviços Web expostos na Internet devem ser hospedados em redes protegidas por Firewall e por infraestruturas de monitorização/bloqueio de tráfego anómalo IPS (Intrusion Prevention System) e IDS (Intrusion Detection System);
- O Ativo TIC deve utilizar mecanismos de proteção contra os ataques cibernéticos do tipo DoS/DDoS (Ataques de negação de serviço ou ataques de negação de serviço distribuída);
- A solução envolvendo o Ativo TIC deve possuir controles para o perímetro de rede e para os pontos de interconexão de tráfego, incluindo internos, como por exemplo: VPC (Private Network), Firewall, IPS, IDS etc.

3.11. Segmentação de Rede

- Ativos de Automação Industrial que compartilham funcionalidades e requisitos de segurança comuns devem ser organizados em zonas de segurança, lógicas e/ou físicas;
- Devem ser estabelecidas configurações com roteamento implementado em Firewall de próxima geração, que determinem que somente a comunicação de aplicações necessárias para a execução das atividades da planta sejam permitidas entre os segmentos, ou seja, o fluxo seja restrito dentro do ambiente Industrial, o qual a norma ISA/IEC 62443 denomina conduíte;
- A segregação física e lógica entre os ambientes Corporativo e Industrial é obrigatória. Sendo assim, não é possível haver compartilhamento de equipamentos entre os ambientes, inclusive de subredes (VLANs). O conceito de restrição de fluxo, contido na norma ISA 62443 deve ser seguido para comunicação na Rede Industrial;
- A Suzano adota estrutura específica, com regras de comunicação bem definidas, entre os diferentes níveis de rede, baseada no modelo PERA (Purdue Enterprise Reference Architecture). Nesta estrutura a ser seguida pela Empresa Prestadora de Serviso devem estar hospedados todos os componentes do ambiente Industrial em suas respectivas subredes (VLANs).

3.12. Segurança Física

- Deve ser mantido um controle de acesso físico nas dependências das Empresas Prestadoras de Serviços, para qualquer usuário, sejam eles: colaborador, visitante etc.;
- Deve-se possuir um sistema de CFTV com gravação e armazenamento das imagens pelo período mínimo de 30 (trinta) dias corridos, de forma On-line;
- Devem ser adotadas proteções preventivas de segurança física em todas as suas dependências, segregando, quando possível, as instalações utilizadas exclusivamente para a prestação do serviço contratado, principalmente quando o serviço utilizar dados confidenciais da Suzano.

3.13. Sistemas de Informação

Os Ativos TIC (doravante, sistemas de informação) das Empresas Prestadora de Serviços são sistemas, plataformas, ferramentas tecnológicas físicas ou lógicas, através dos quais as informações da Suzano são tratadas. A partir desse conceito, a Empresa Prestadora de Serviços deve:

- Disponibilizar à Suzano todas as versões e pacotes principais do Software que compõe a Solução contratada;
- Manter as instalações onde são mantidos os sistemas de informações protegidas e com acesso controlado;
- Garantir que todo usuário possui credencial de acesso individual, com um ID único, devendo manter o histórico de todas as atividades realizadas por essa credencial;
- Utilizar credencial de acesso M2M (Machine to Machine) apenas para caráter de Troubleshooting, quando aplicável, de forma controlada e efetuando a troca da senha após o uso;
- Atribuir aos perfis de autorização definidos, para acesso aos dados do Ativo TIC, os conceitos Need to Know e Least Privilege, além de aplicar a segregação de funções (SoD). Os perfis devem ser configurados antes do início do tratamento, para que seja documentado e associado para cada usuário ou para um conjunto de usuários que vão executar a mesma função;
- Realizar revisão periódica de credenciais e perfis de acesso aos sistemas de informação;
- Os acessos dos usuários que não estiverem mais atribuídos a Suzano ou que não precisam mais acessar os dados da Suzano, devem ser removidos imediatamente, com a finalidade de impedir acessos não autorizados. Deve ser garantido:
    - Remoção por tempo de inatividade;
    - Remoção na data de expiração prevista, ao menos que seja estendida por solicitação da Suzano;
    - Bloqueio do acesso após tentativas incorretas;
    - Bloqueio quando na identificação do uso ilegal ou quando colocado em risco a segurança da informação;
    - Bloqueio por solicitação da Suzano.
- Implementar um padrão de senha forte, utilizando o duplo fator de autenticação, para os acessos realizados;
- Garantir que todo Software instalado deve ser legalmente licenciado;

- Possuir antivírus atualizado, sempre que houver novas versões disponíveis;
- Manter atualizado os sistemas operacionais e aplicações, conforme recomendações de segurança do padrão OWASP, sempre que aplicável;
- Modificar e deletar configurações padrão do sistema de informação, como senhas, portas, contas de serviços, etc. aplicando o Hardening, de acordo com as recomendações do fabricante;
- Implementar controles e práticas de segurança adequados para proteger todas as interfaces de comunicação utilizadas nos serviços contratados. Tais medidas devem incluir mecanismos fortes de autenticação, autorização e criptografia, reconhecidos pelas melhores práticas de mercado;
- Aplicar a mitigação de vulnerabilidades catalogadas, de acordo com os padrões de mercado;
- Proteger todo o ambiente por Firewall e IDS (Intrusion Detection System), assim como ter as devidas segregações de redes, com a finalidade de proteger a infraestrutura, deixando exposto apenas o Front-End e a camada de exposição. É imprescindível que os sistemas de informação expostos na Internet possuam WAF (Web Application Firewall) e soluções de proteção de negação de serviço (DoS/DDoS);
- Adotar processos adequados de Backup e Restore quando houver tratamento de dados da Suzano, em acordo com o gestor do contrato. O processo deve ser documentado e deve conter pelo menos a indicação da frequência, dos métodos de execução, do arquivamento e da retenção dos Backups, incluindo teste de Restore;
- Informações da Suzano devem ser mantidos apenas durante a vigência de contrato. Quando aplicável, os Backups devem ser entregues a Suzano e deve ser garantido o descarte correto de toda informação de propriedade ou controle da Suzano;
- Todas as soluções que possuem dados da Suzano devem ser segregadas entre os ambientes de produção e homologação, de forma que sejam alocados em infraestruturas distintas, físicas e virtuais;
- Implementar procedimentos operacionais específicos para execução das atividades de restauração, quando aplicável, incluindo o tempo de implementação acordados com o gestor do contrato e a garantia da continuidade do serviço contratado pela Suzano, quando na ocorrência de um incidente de segurança da informação nos sistemas de informação;
- Criptografar as informações confidenciais que são processadas, armazenadas e transmitidas pelos sistemas de informação que mantém informações da Suzano, para que seja garantindo a proteção das informações;
- Implementar rastreamento dos usuários e administradores nos sistemas de informação, visando a coleta e armazenamento de registros de acesso (Login/Logout) e as demais ações realizadas, mantendo a integridade, não repetibilidade e não repúdio. A rastreabilidade dos acessos das ações deve ser mantida pelo período mínimo de 12 (doze) meses;
- Os sistemas de informação, quando aplicável, devem passar por análise de vulnerabilidade e teste de invasão antes da sua entrada em ambiente de produção e devem ser avaliados periodicamente, mesmo quando em ambiente de produção.

3.14. Uso Seguro de Inteligência Artificial (IA)

É imprescindível que a EPS tenha políticas internas e controles quanto ao uso de dados da Suzano em Soluções de IA próprias ou terceiras para, por exemplo: criação de relatórios, ajustes em documentação, geração de Insights etc.
Caso a EPS forneça à Suzano Soluções baseadas em IA, os requisitos abaixo, além dos demais requisitos presentes neste documento, devem ser seguidos para garantir a segurança dos dados tratados, seguem:

- Deve ser garantido que somente os dados estritamente necessários e autorizados pela Suzano, são coletados e utilizados pela Solução de IA;
- Deve existir segregação de função e de ambientes com restrição ao acesso aos dados e modelos de IA;
- Modelos devem ser protegidos contra extração, inversão ou engenharia reversa;
- Devem ser implementados mecanismos para detectar e mitigar inputs maliciosos que alterem o comportamento dos modelos de IA utilizada;
- Modelos pré-treinados devem ser avaliados quanto à segurança da informação e confiabilidade antes da utilização;
- Modelos e Soluções de IA, com componentes próprios ou de terceiros, devem ser testados quanto a presença de vulnerabilidades e atualizados com processos seguros e controlados.

3.15. Wi-Fi Suzano S.A.

O acesso ao Wi-Fi Suzano é disponibilizado aos usuários, a partir das suas dependências, sendo dedicado às atividades laborais. No entanto, não é permitido determinadas ações, como:

- Não deve ser instalado ponto de acesso pessoal na rede da Suzano para configurar uma rede Wi-Fi paralela. A conexão a serviços Wi-Fi só é permitida por meio do Wireless, utilizando infraestrutura da Suzano;
- Não deve ser realizada qualquer atividade que possa trazer dano ao serviço ou a infraestrutura da rede Suzano. Seguem algumas atividades ilegais, porém não estão limitadas apenas a estas: varredura de portas, varredura de vulnerabilidades, identificação de senhas, Sniffing, Spoofing, descoberta de rede, Fingerprinting, Footprinting, Pentest, redirecionamento ou modificação de tráfego etc.