## 1. OBJETIVO

A Política de Privacidade da Kepler Weber S/A, e suas controladas, inscrita no CNPJ sob o número 91.983.056/0001-69, com sede na Rua do Rócio, nº. 84, 3º Andar, Bairro Vila Olímpia, São Paulo/SP, CEP 04.552-000, que, para fins da presente política será mencionada como **Kepler Weber**, tem por propósito estabelecer diretrizes sobre Segurança da Informação, bem como estabelecer padrões de comportamento seguro, adequados às metas e necessidades da Kepler Weber. As diretrizes buscam proteger informações, inclusive os dados pessoais no ambiente da Kepler Weber, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

## 2. ABRANGÊNCIA

Esta política é aplicada a todos os usuários da informação da Kepler Weber, incluindo qualquer indivíduo ou organização que possui vínculo com a Kepler Weber, isto é, colaboradores, membros da alta direção, parceiros de negócios e terceiros contratados pela Kepler Weber.

## 3. DEFINIÇÕES

**Ameaça**: Causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou à organização**.**

**Ativo:** Tudo aquilo que possua valor para a organização, desde hardware, software, serviços impressos (papéis), mas também em pessoas, habilidades, experiências, bem como reputação e imagem.

**Membros da Alta Direção:** Pessoas físicas que tenham o poder de gestão sobre os negócios da Kepler Weber, por exemplo: membros do Conselho de Administração, membros do Conselho Diretor, membros da Diretoria, membros do Conselho Fiscal e membros do Comitê Executivo.

**Confidencialidade:** Propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos.

**Controle:** Meios de gerenciar o risco, incluindo políticas, procedimentos, diretrizes e práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modifiquem o risco à Segurança da Informação.

**Disponibilidade:** Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.

**Gestor da Informação:** Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a sua responsabilidade.

**Incidente de segurança da informação:** É indicado por um único ou uma série de eventos de segurança da informação, indesejáveis ou inesperados, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameaçam a segurança da informação.

**Integridade:** Permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente.

**Não repudio:** Habilidade de provar a ocorrência de um suposto evento ou ação e suas entidades.

**Política:** A intenção e orientação geral formalmente expressa pela alta administração.

**Risco:** Efeito da incerteza sobre os objetivos de segurança da informação da Kepler Weber.

**Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da Kepler Weber.

**Usuário:** Empregados com vínculo empregatício de qualquer área da Kepler Weber ou terceiros alocados na prestação de serviços à Kepler Weber, indiferente do regime jurídico a que estejam submetidos.

**Vulnerabilidade:** Fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças.

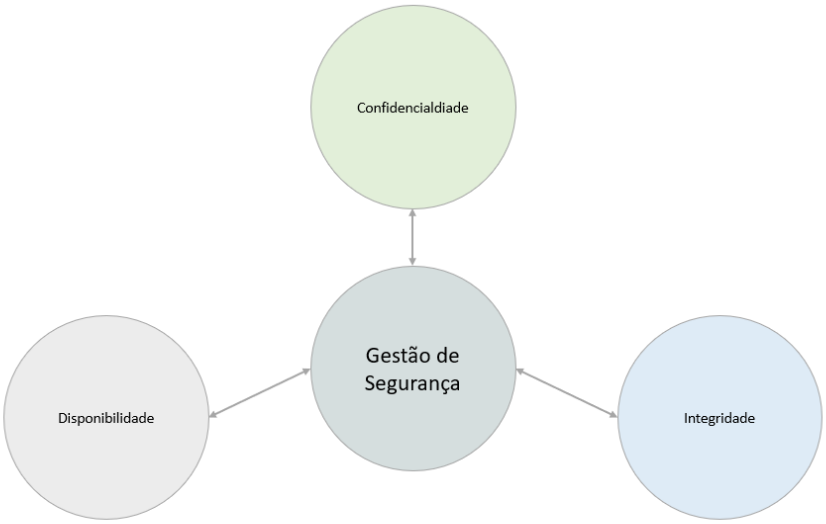
## 4. INFORMAÇÃO DOCUMENTADA

O documento será armazenado no dispositivo eletrônico abaixo discriminado:

| Área: | | | | | |
|---|---|---|---|---|---|
| **Nº** | **IDENTIFICAÇÃO** | **ARMAZENAMENTO (local) RECUPERAÇÃO (ordem)** | **PROTEÇÃO (forma de arquivamento)** | **TEMPO DE RETENÇÃO** | **DISPOSIÇÃO** |
| 1. | POCA 015 | SESuit | Eletrônico | Indeterminado | n/a |

## 5. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Toda informação recebida ou produzida pelos profissionais da Kepler Weber como resultado de atividades profissionais são da companhia. Exceções poderão ser aplicadas caso a caso e devem ser devidamente formalizadas em ata pelo Comitê de Segurança da Informação.




Os sistemas, equipamentos físicos ou ferramentas do dia-a-dia de trabalho devem ser utilizados seguindo a conduta profissional prevista no Código de Conduta da Kepler Weber.

Com isso, os princípios de segurança das informações são elementares para a execução de trabalhos, buscando garantir a disponibilidade, integridade e a sua confidencialidade. Estes princípios devem ser considerados com o objetivo de minimizar riscos de perdas ou violação de informações e, ainda, de dados pessoais que fazem parte da Kepler Weber.

### 5.1. Compromisso da Kepler Weber

A Kepler Weber, por meio desta política, espera conscientizar os profissionais e terceiros e evitar a materialização de perdas de informações pela quebra de princípios. Adicionalmente, minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da Kepler Weber como resultado de falhas de segurança.

## 6. MEDIDAS DE SEGURANÇA

A Kepler Weber, tem como missão produzir e entregar soluções inovadoras de pós-colheita, gerar valor para clientes, acionistas, parceiros de negócios.

A alta administração da Kepler Weber está comprometida com uma gestão efetiva de segurança da informação, apoiando para o cumprimento desta política e procedimentos a ela relacionada.

O objetivo da Segurança da Informação da Kepler Weber é garantir a gestão efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte a ambientes críticos do negócio, mitigando riscos e identificados seus eventuais impactos às operações da Kepler Weber.

A seguir serão apresentadas medidas de segurança a fim de minimizar os riscos de perda, vazamento, acessos indevidos a informações da Kepler Weber. Ressaltamos que tais medidas são formas para evitar que as informações sofram alguma infração aos princípios, mas esperamos que você como profissional aja com a conduta esperada no uso de informações.

### *6.1 Criptografia*

A Kepler Weber adota controles criptográficos, bem como regras para uso de chaves criptográficas, a fim de proteger a confidencialidade, a integridade, a autenticidade e o não repudio das informações, seguindo as boas práticas do NIST e 27001, utilizando softwares e protocolos seguros para criptografia de dispositivos e comunicação.

### *6.2 Backup*

O procedimento de backup segue as boas práticas da NBR ISO/IEC 17799 da ABNT, com controle de armazenamento dos dados, manutenção do hardware utilizado para o armazenamento e nomenclatura dos arquivos. O backup é realizado de forma automatizada seguindo os controles de segurança da informação sendo eles: proteção física e ambiental, localidade remota, registro e documentação, criptografia e confidencialidade, recuperação de desastres e período de retenção.

O backup tem por objetivo manter a disponibilidade e a continuidade das informações.

### *6.3 Gestão de acessos, identidades e perfis*

A fim de garantir a confidencialidade de informações a Kepler Weber conta com mecanismos de tecnologia da informação capazes de impedir que pessoas não autorizadas acessem informações confidenciais ou com restrições por área de negócio.

A informação só pode ser acessada e atualizada por pessoas autorizadas e devidamente credenciadas, cujo gerenciamento é realizado pela Kepler Weber. Dados e informações importantes de alguns setores ou clientes jamais podem ser acessados por terceiros estranhos à corporação.

A Kepler Weber realiza atividades de restrições de acesso entre áreas de negócio para evitar eventuais acessos indevidos.

A Kepler Weber dispõe de Procedimento de Gestão de Identidade e Perfis, que trata do rigoroso controle de segurança para utilização de senhas no ambiente corporativo, disponível para todos colaboradores, membros da alta direção, parceiros de negócios e terceiros da Kepler Weber, no SESuit.

### *6.4 Senhas*

No Procedimento de Gestão de Identidade e Perfis mencionado acima, é prevista a utilização de senha para acessar os sistemas internos, a qual requer critérios mínimos, quais sejam: utilização caracteres especiais, quantidade mínima de carácteres e demais controles informados pela área de tecnologia da informação.

### *6.5 Uso de dispositivos eletrônicos*

Os equipamentos fornecidos aos colaboradores são de propriedade da Kepler Weber, cabendo a cada profissional utilizá-los e manuseá-los de maneira adequada para executar suas atividades de trabalho e de interesse da companhia, bem como cumprir as recomendações da área de tecnologia da informação.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da área de Tecnologia da Informação da Kepler Weber, ou de quem este determinar.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação pelo time de Tecnologia da Informação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os computadores e seus respectivos sistemas para uso possuem versões do software antivírus instaladas, ativadas e atualizadas permanentemente.

No caso de suspeita de vírus ou problemas na funcionalidade, o usuário deve acionar o departamento técnico responsável mediante registro de chamado no Service Desk.

Arquivos pessoais e/ou não pertinentes ao negócio da Kepler Weber (fotos, músicas, vídeos, etc.) não são permitidos. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente, sem a necessidade de comunicação prévia ao usuário.

O acesso à páginas web (Internet) dentro do ambiente Kepler Weber é efetuada através de controles adotados pela Segurança da Informação segmentado por função, instalação de Softwares nos dispositivos disponibilizados pela Kepler Weber.

A utilização de dispositivos pessoais, no ambiente da Kepler Weber, deverá ser precedida de autorização da gestão imediata, e a instalação ou aprovação para instalação de software deverá seguir os procedimentos internos da área Tecnologia da Informação.

### *6.6 Boas práticas de uso do e-mail corporativo*

O uso do e-mail corporativo da Kepler Weber é uma ferramenta de comunicação profissional em que torna o colaborador um representante da empresa, além de identificá-lo.

Ao utilizar o e-mail corporativo o colaborador deve utilizá-lo para:

- Fins profissionais;
- Si próprio em nome da companhia, não podendo compartilhar seus acessos com outras pessoas (colaboradores da Kepler Weber ou não).

A Kepler Weber adota como boas práticas, para utilização de e-mail corporativo, o controle de armazenamento, backup, monitoramento de envio e recebimento de mensagens eletrônicas, filtros anti-spam e a utilização de firewall/antivírus, orientação aos colaboradores, identificação de e-mails como “interno” ou “externo” à sua rede, além de adotar controles de segurança como softwares e hardwares para garantir a integridades dos seus dados que circulam dentro e fora do seu ambiente corporativo.

### *6.7 Das obrigações da Kepler Weber*

6.7.1 Elaborar, implementar e seguir por completo as políticas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da Kepler Weber sejam atingidos através da adoção de controles de segurança da informação contra ameaças provenientes de áreas internas e externas.

6.7.2 Disponibilizar políticas, normas e procedimentos de segurança da informação a todas as partes interessadas, sendo também de conhecimento de todos: colaboradores, membros da alta direção, parceiros de negócios e terceiros.

6.7.3 Assegurar a educação e conscientização sobre as práticas adotadas pela Kepler Weber de segurança da informação para colaboradores, membros da alta direção, parceiros de negócios e terceiros.

6.7.4 Atender integralmente os requisitos de segurança da informação aplicáveis ou exigidos por legislação, normas e regulamentações nacionais e internacionais.

6.7.5 Tratar imediatamente e totalmente qualquer evento de segurança da informação que possa vir impactar o ambiente de negócio da Kepler Weber, garantindo que eles sejam

registrados, classificados, investigados, corrigidos, documentados, e quando necessário, efetuar comunicação aos órgão reguladores;

6.7.6 Garantir a continuidade do negócio através da adoção, implementação, testes e melhoria contínua de planos de continuidade e recuperação de desastres;

### *6.8 Auditoria de Segurança da Informação*

Trata-se de uma avaliação sistemática da segurança do sistema de informações, medindo o quanto ele está em conformidade com um conjunto de critérios estabelecidos pela companhia. Essa avaliação contempla a segurança da configuração da infraestrutura, do ambiente, dos sistemas, de softwares, dos processos de manipulação de informações e de práticas dos usuários.

A Kepler Weber executa, rotineiramente, por meio de empresa terceirizada, auditoria nos processos de segurança e tecnologia da informação, que compreende a análise de configurações de sistemas operacionais, compartilhamentos de redes, varredura de vulnerabilidade, aplicações, softwares, sistemas, processos, dados históricos, acessos e consciência dos usuários, bem como, busca medir a conformidade dos sistemas com os critérios estabelecidos pela companhia, para garantir que processos e infraestrutura estejam permanentemente atualizados.

### *6.9 Atribuições e Responsabilidades*

#### *6.9.1 Comitê Gestor de Tecnologia da Informação (CGTI)*

O Comitê Gestor de Tecnologia da Informação, criado em Reunião de Diretoria realizada em 23.02.2021, é órgão colegiado de natureza consultiva e propositiva, de caráter permanente. Tem por finalidade suportar a Gerência de TI na governança de recursos de Tecnologia de Informação, visando estabelecer as prioridade e as principais diretrizes organizacionais.

O CGTI é formado pelas gerências das áreas de tecnologia da informação, suprimentos, controladoria, comercial, gente e gestão, produção e logística, implantação de projetos, jurídico, governança e compliance, pelo coordenador de inovação e pelo analista de insfraestrura sênior.

As atribuição e responsabilidade do CGTI estão regulamentadas em documento específico, anexo a ata RD 005-2021 de 23/02/2021.

#### *6.9.2 Analista de Segurança da Informação*

São responsabilidade do analista de segurança da informação:

6.9.2.1 Conduzir a operação da segurança da informação, tendo como base esta política e demais políticas, normas e procedimentos;

6.9.2.2 Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação necessários para se fazer cumprir esta política;

6.9.2.3 Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implementar medidas corretivas para mitigar o risco e dar continuidade ao negócio.

6.9.2.4 Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento imediato e adequado.

6.9.2.5 Preservação da confidencialidade, integridade e disponibilidade da informação, tais como autenticidade, responsabilidade, não repúdio.

#### *6.9.3 Gestores da Informação*

Gestores da informação são os responsáveis pelo tratamento da informação em suas respectivas áreas. São responsabilidades dos gestores da informação:

6.9.3.1 Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme procedimentos estabelecidos pela área de Segurança da Informação.

6.9.3.2 Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela Kepler Weber;

6.9.3.3 Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas caso necessário;

6.9.3.4 Autorizar e revisar os acessos à informação e sistemas de informação, dos usuários sob sua responsabilidade;

6.9.3.5 É responsabilidade do gestor imediato, seguir as normas e procedimentos vigentes para devolução dos equipamentos disponibilizados pela Kepler Weber.

6.9.3.6 Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com o Procedimento de Gestão de Acessos da Kepler Weber**.**

***6.9.4 Usuários da informação***

Usuários da informação da Kepler Weber são os colaboradores, membros da alta direção, parceiros de negócios e terceiros, que possuam acesso aos sistemas, banco de dados, documentos físicos e eletrônicos de propriedade da Kepler Weber. São responsabilidades dos usuários das informações da Kepler Weber:

6.9.4.1 Ler, compreender e cumprir integralmente os termos desta Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

6.9.4.2 Encaminhar qualquer dúvida ou pedido de esclarecimento sobre a Política Segurança da Informação, suas normas e procedimentos à área de Segurança da Informação, através do e-mail segurancadainformacao@kepler.com.br;

6.9.4.3 Comunicar qualquer evento que viole esta Política e/u que possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da Kepler Weber;

6.9.4.4 Assinar o Termo de Confidencialidade da Kepler Weber, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos vigentes da Kepler Weber, assumindo total responsabilidade pelo seu cumprimento;

6.9.4.5 Responder por não cumprir a Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

## 6.10 Sanções e Punições

A violação de quaisquer princípios e vedações desta Política sujeita o colaborador, membro da alta direção, administrador ou conselheiro às sanções disciplinares, correspondendo à gravidade da infração, prevista em política própria de medidas disciplinares.

## 6.11 Disposições Finais

A presente política passa a vigorar para todos os colaboradores, membros da alta direção, terceiros, fornecedores e parceiros de negócios da Empresa, após a aprovação do Conselho de Administração, em 15 (quinze) dias a contar da data de publicação na plataforma do SESuit e no site corporativo https://www.kepler.com.br/governanca/politicas-kw.

Esta norma substitui todas as normas internas vigentes sobre o assunto que eventualmente se contraponham ao que foi aqui estabelecido.

A Empresa pode, por sua mera liberalidade ou em razão de alterações legislativas, a qualquer momento, e deve a cada 2 (dois) anos revisar os termos da presente política, sendo que em caso de alteração será submetido a nova aprovação.

Este instrumento é parte integrante do contrato de trabalho existente entre o colaborador e a Kepler Weber, tendo a presente vigência válida enquanto vigente o contrato de trabalho.

Quaisquer omissões, interpretações e exceções deverão ser levadas à apreciação e decisão do Comitê de Integridade.

## 7. CONTROLE DE ALTERAÇÕES

| REVISÕES | DESCRIÇÃO DAS ALTERAÇÕES | DATA |
|---|---|---|
| | | |
| | | |

## 8. ANEXOS

**TERMO DE ACEITE**
**Política de Segurança da Informação**

DS

Eu, _____, matrícula KW nº _____, estou ciente das diretrizes e obrigatoriedade da preservação da confidencialidade e sigilo profissional em relação às informações que possuo acesso dentro do ambiente Kepler Weber, inclusive após o encerramento de minhas atividades junto a Kepler Weber, fornecedores e clientes. Estou ciente que a área de Tecnologia da Informação (TI) reserva-se o direito de realizar auditorias e monitorações a qualquer momento nas atividades executadas por colaboradores e prestadores de serviços.

Declaro conhecer a Política de Segurança da Informação a qual comprometo-me a cumprir em sua totalidade, mesmo quando ocorrer a execução de trabalhos fora das instalações da empresa. Também me comprometo a não reproduzir quaisquer documentos, dados ou informações da organização sem o expresso consentimento desta, através de autorização de representante com poderes para tanto.

Afirmo ter recebido orientações quanto ao uso dos equipamentos disponibilizados para execução de minhas atividades, sendo elas:

a) Todos os recursos computacionais da empresa são fornecidos para propósitos de negócio. O uso de qualquer recurso para outras finalidades é estritamente proibido;
b) Não é permitido ao colaborador/prestador desrespeitar padrões definidos da empresa, quebrar senhas de segurança, instalar software não homologado pela equipe de TI ou modificar configurações e caracteristcas dos equipamentos sem o consentimento do setor de Tecnologia da Informação, sendo proibido compartilhamento de senha;
c) Não é permitido ao colaborador/prestador alterar características originais do equipamento, bem como realizar manutenções não autorizadas pela equipe responsável de TI;
d) No caso dos dispositivos cedidos pela empresa para apoio a execução das atividades, a responsabilidade em relação à preservação da segurança física e lógica, integridade, confidencialidade, acesso e uso de ativos de informações da empresa é integralmente do colaborador/prestador que utiliza o equipamento;
e) Garantir a segurança e integridade física do equipamento, protegendo contra exposição a campos magnéticos, conforme as especificações do fabricante;
f) Reportar os incidentes de segurança da informação, suspeitos ou confirmados, através dos canais disponibilizados pela TI ou através do Canal de Ética;
g) Os colaboradores/prestadores são responsáveis por comunicar de imediato a seu superior hierárquico quaisquer irregularidades relacionadas aos itens mencionados acima. O não cumprimento deste

documento pode ser razão para a aplicação da legislação cabível no território nacional por questões de propriedade intelectual.

_____/____, de _____de 202__.

_____

Nome:

CPF: