CARTILHA DE:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

alibra

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A presente Política de Segurança da Informação tem por objetivo o gerenciamento das informações da **ALIBRA INGREDIENTES S.A.** Assim, deverá ser seguida por todos os seus colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviços.

A responsabilidade em relação à segurança da informação deve ser comunicada no início do vínculo com a ALIBRA INGREDIENTES S.A, devendo os empregados e prestadores de serviços assinar o Termo de Responsabilidade e Confidencialidade, de forma manual ou eletrônica. na forma do Anexo I, parte integrante desta Política.

1.1. CONFIDENCIALIDADE

Os colaboradores, sem exceção, deverão observar as regras de confidencialidade. Todo Colaborador a quem se conceda acesso a informações confidenciais deve ser identificado nos termos do item 1.4, abaixo, e, nesta condição, respeitar todos os procedimentos determinados nesta e demais Políticas da Empresa. Apenas pessoas autorizadas terão acesso à informação confidencial, e apenas na medida do necessário para a execução de suas atividades.

Caso um detentor de informação confidencial mude de função dentro da empresa na qual o acesso a tal informação não seja mais necessário, o superior hierárquico do colaborador deverá informar ao responsável de Tecnologia para que o acesso do colaborador seja restringido.

Da mesma forma, no ato do desligamento de um colaborador, o acesso deste a todos os sistemas, informações e documentos da empresa será bloqueado.

1.2. CONTROLE DE INFORMAÇÕES

Os colaboradores que detenham Informações Confidenciais, em função de seus cargos ou atribuições na empresa, devem manter a descrição e a confidencialidade para os demais colaboradores e as seguintes condutas devem ser observadas:

1.2.1. Os colaboradores devem evitar levar para ambientes externos à empresa cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, devendo essas cópias serem criptografadas ou mantidas através de senha de acesso;

1.2.2. Os documentos descartados devem ser destruídos, de forma a garantir que informações relevantes não sejam repassadas a terceiros;

1.2.3. O descarte de informações confidenciais e dados pessoais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação da equipe de TI;

1.2.4. As informações e os dados pessoais que possibilitem a identificação de um cliente ou colaborador da empresa devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressos se forem para o atendimento às atividades profissionais;

1.2.5. Os colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da empresa, como por exemplo vírus, fraudes, vazamentos etc.; e

1.2.6. Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos.

1.3. IDENTIFICAÇÃO DOS COLABORADORES DETENTORES DA INFORMAÇÃO, MANUTENÇÃO DE REGISTROS E LOGS

A empresa manterá o registro dos colaboradores que detenham Informações Confidenciais, com a indicação do tipo de informação detida, separadas por pastas com acesso liberado pelo gestor responsável, devendo informar ao departamento responsável e para a diretoria todas as Informações confidenciais que estejam em poder dos colaboradores que possam significar restrição nas operações da empresa.

Será atribuído a cada conta ou dispositivo de acesso a sistemas, bases de dados e qualquer outro ativo de informação, um responsável identificável como pessoa física, sendo que os usuários (*login*) individuais de colaboradores internos serão de responsabilidade do próprio colaborador e os usuários (*login*) de terceiros serão de responsabilidade do diretor da área contratante. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

Com relação ao monitoramento e auditoria do ambiente, a empresa possui sistemas de monitoramento, servidores, correio eletrônico. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como

material manipulado.

A empresa poderá tomar as seguintes medidas:

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou por solicitação da Diretoria;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; ou
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.
- Instalar sistemas de rastreamento e monitoramento de estações móveis de trabalho com a possibilidade de remoção remota de todos os arquivos no caso de perda ou roubo do dispositivo.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da empresa e sujeitará o usuário às sanções administrativas e legais cabíveis, observado o disposto no item que trata de Sanções, constante do Código de Conduta da Empresa.

A título de informação, segue lista orientativa e não exaustiva de eventuais situações que são passíveis de sanções: uso ilegal de software; introdução (intencional ou não) de vírus em equipamento de informática; tentativas de acesso não autorizado a dados e sistemas; divulgação de informações confidenciais da Empresa.

1.4. PROTEÇÃO DA BASE DE DADOS

Os recursos de informática da Empresa devem:

- ser protegidos contra adulterações; e
- permitir a realização de auditorias e inspeções.

Todos os registros eletrônicos realizados pela empresa deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos públicos como por exemplo a ANPD.

As informações mantidas em meios eletrônicos devem possuir políticas de backup periódicos e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso a essas bases deve ser limitado somente a pessoas autorizadas pela área de T.I. ou pela diretoria.

1.5. VAZAMENTO DE DADOS PESSOAIS E INFORMAÇÕES CONFIDENCIAIS

Os colaboradores deverão comunicar à área de T.I. e à diretoria quaisquer casos de violações

às normas de segurança da informação que tenham conhecimento. Toda violação ou desvio deve ser investigado para a determinação de medidas necessárias, visando à correção da falha ou reestruturação de processos. Em caso de vazamento de dados pessoais e informação confidencial, a Diretoria discutirá com o Comitê de Privacidade *e* com o Responsável pela Segurança da Informação sobre o plano efetivo de recuperação e medidas para minimizar e prevenir danos.

1.6. TREINAMENTO DE SEGURANÇA DA INFORMAÇÃO E TESTES PARA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

A empresa realizará testes periódicos de segurança para os sistemas de informações eletrônicos ou não, anualmente, visando reduzir riscos de perda informações e dados pessoais, de confidencialidade, integridade e disponibilidade dos ativos de informação.

O treinamento sobre segurança de informação fará parte do treinamento inicial e periódico da Empresa, que deverá assegurar que todos os colaboradores tenham conhecimento dos procedimentos e das obrigações aqui previstos, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos.

1.7. POLÍTICA PARA DISPOSITIVOS PESSOAIS

Os colaboradores deverão comunicar ao Departamento de Recursos Humanos e Departamento de TI sua opção por utilizar seus dispositivos pessoais (BYOD – *bring your own device*), como smartphones e laptops, para acesso à rede corporativa, sistemas internos e bancos de dados e a empresa decidirá sobre o uso ou não te tais dispositivos.

Se autorizado o uso de equipamentos pessoais, esses dispositivos BYOD devem ser constantemente monitorados pela empresa. Esse monitoramento é importante para ter conhecimento de possíveis violações à política de segurança, incidentes e poder tomar ações preventivas.

A área de T.I. auditará o dispositivo, e poderá instalar ferramentas de monitoramento e remoção remota de informações (para caso de roubo ou perda do dispositivo) e somente aprovará seu uso se o Colaborador concordar em:

- Acompanhar treinamentos de segurança promovidos periodicamente pela área de T.I.*;*
- Aprovar a gestão de soluções móveis da empresa, que contém, dentre seus principais termos, os seguintes pontos:

- Ações para bloqueamento remoto,
- Remoção completa de arquivos,
- Restauração aos padrões de fábrica,
- Monitoramento constante de atividades realizadas no dispositivo;

- Possuir solução antivírus ou malware;
- Seguir os procedimentos definidos nesta política em casos de incidentes como perda, furto, roubo ou extravio dos dispositivos pessoais que possam ter sido usado para realizar qualquer tarefa relacionada a empresa;
- Utilizar sempre a versão mais atualizada do sistema operacional e efetuar todas as atualizações do fabricante;
- Não utilizar logins pessoais para qualquer tarefa relacionada à empresa;
- Não emprestar o dispositivo para terceiros, inclusive membros da família;
- Não instalar aplicativos não oficiais ou não homologados pela empresa;
- Não usar redes de Wi-Fi públicas;

- Nunca clicar em links ou abrir anexos de e-mails de fontes não confiáveis para evitar *phishing;*
- Entregar o dispositivo à área de T.I, no caso de desligamento, para reconfiguração e limpeza de dados da empresa;

1.8. RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO

O Departamento de T.I. é o responsável pela segurança da Informação na empresa.

As funções e reponsabilidades do setor responsável pela segurança da Informação são:

- Testar a eficácia dos controles utilizados e informar a Diretoria sobre eventuais riscos residuais.
- Estabelecer o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança da empresa, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada usuário e reduzir o número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de

negócio.

- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar as informações dos ativos da Empresa.
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da Empresa, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável pela Segurança da Informação que deverá comunicar à Diretoria.

1.9. ATRIBUIÇÕES E RESPONSABILIDADES

Caberá a todos os colaboradores conhecer e adotar as disposições das Políticas de Segurança da Informação, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas.

Em caso de incidente que afete a Segurança da Informação da empresa, o colaborador deverá comunicar imediatamente ao Departamento de T.I. Em caso de descumprimento, estará sujeito às sanções internas aplicáveis e a responsabilização na forma da lei.

1.10. IDENTIFICAÇÃO/AVALIAÇÃO DE RISCOS (*RISK ASSESSMENT*)

A empresa periodicamente deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido pela equipe de TI, o qual deverá ser documentado com o objetivo de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da empresa. A Empresa poderá contratar uma empresa terceirizada, caso o Responsável pela Segurança da

Informação, julgue necessário e mediante aprovação da Diretoria.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, documentados, implantados e testados durante a fase de execução.

Abaixo, listamos riscos de segurança cibernética identificados, na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”);
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em desconformidade com as condições estabelecidas nesta Política;
- Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais ou informações de clientes, como pharming, phishing, vishing e smishing;
- Não conformidade com a política de BYOD; ou
- Vazamento de informações durante tráfego de dados não criptografados.

Periodicamente a empresa deverá revisar o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança de cibersegurança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

1.11. AÇÕES DE PREVENÇÃO E PROTEÇÃO

A empresa estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. O colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

1.12. INTERNET, E-MAIL E COMPUTADORES

A empresa oferece a seus colaboradores uma completa estrutura tecnológica para o exercício das atividades. É de responsabilidade do colaborador manter e zelar pela integridade dessas ferramentas de trabalho.

Além disso, o colaborador é responsável pela proteção de seu banco de dados, seja ele composto por planilhas, e-mails e/ou comunicação telefônicas contendo dados confidenciais de clientes e/ou da empresa dentre outros.

- Os equipamentos e computadores utilizados pelos colaboradores devem ser utilizados com a finalidade exclusivamente profissionais e sob nenhuma hipótese servirão de instrumento à discriminação em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei;
- A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da empresa, depende de autorização expressa do Responsável pela Segurança da Informação e deverá observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes;
- Os downloads de qualquer natureza devem ser feitos com diligência por parte do usuário, para fins exclusivamente profissionais. Periodicamente e sem aviso prévio serão realizadas inspeções nos computadores para averiguação de *downloads* impróprios não autorizados ou gravados em local indevido;
- O e-mail disponibilizado pela empresa caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo de utilização exclusivamente profissionais;
- As mensagens enviadas ou recebidas através do correio eletrônico corporativo (os “e-mails corporativos”), seus respectivos anexos, e a navegação através da rede mundial de computadores (a “Internet”) através de equipamentos da empresa são monitoradas;
- Os e-mails Corporativos recebidos pelos Colaboradores, quando abertos, deverão ter sua adequação às regras desta Política. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem;

- Nos equipamentos e computadores disponibilizados pela empresa não é recomendado o uso de e-mails públicos (*webmails*) ou qualquer outro tipo de correio eletrônico que não seja o correio corporativo da empresa. Fica também proibido a utilização de programas de conversas eletrônicas (CHATs) externos, gratuitos ou não, salvo para fins comerciais, quando autorizado pelo Responsável pela Segurança da Informação.

1.13. SENHAS

A senhas são de caráter sigiloso, pessoal e intransferível serão fornecidas aos colaboradores para acesso à rede corporativa, sistemas internos e ao correio eletrônico corporativo. Em nenhuma hipótese as senhas deverão ser transmitidas a outras pessoais, sendo os colaboradores responsáveis pela manutenção de suas senhas.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras passiveis de engenharia social.

1.14. MONITORAMENTO TELEFÔNICO

As conversas telefônicas originadas ou recebidas pelo sistema de telefonia da empresa poderão ser monitoradas e gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política, inclusive no âmbito judicial.

1.15. MONITORAMENTO POR CÂMERAS

A empresa utiliza um serviço de monitoramento por câmeras e são gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política.

1.16. PROCEDIMENTOS DE SEGURANÇA PARA TERCEIROS

Os colaboradores externos da empresa, dentre os quais os seus fornecedores, prestadores de

serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de colaboradores externos, envolve determinados riscos que devem ser levados em conta pela empresa, demandando certos cuidados proporcionais a esta identificação de ameaças.

1.16.1. AVALIAÇÃO DOS TERCEIROS CONTRATADOS

A contratação de terceiros se pautará, no que tange à segurança da informação e conforme se verificará em diligência específica, pelos seguintes critérios:

- O terceiro deve possuir políticas, programa e procedimentos formais relativos à segurança da informação que sejam auditados e atualizados periodicamente.
- O terceiro deve possuir plano de resposta a incidentes de segurança da informação;
- O terceiro deve realizar, em medida adequada, ações de conscientização, educação e formação de segurança de seus empregados.
- O terceiro deve possuir, comprovadamente, mecanismos satisfatórios para proteção dos dados transacionados com a empresa. O terceiro deve possuir responsável técnico e deter sistemas e políticas satisfatórias para detecção e reporte de atividades não autorizadas nos sistemas utilizados em sua relação com a empresa.
- O terceiro deve possuir canal adequado para o reporte completo e tempestivo de incidentes de segurança da informação, assim como determinar em suas políticas as hipóteses de comunicação de tais

  incidentes a clientes e/ou reguladores, quando aplicável.
- O terceiro deve possuir política formalizada de segurança da informação, e deve manter sempre vigentes e regulares todas as suas certificações necessárias à prestação dos serviços contratados.

Nesse sentido, a área de T.I. deverá verificar o conteúdo mínimo de segurança da informação de terceiros que:

- Possuem acesso a dados e informações e sistemas confidenciais ou sensíveis,
- prestem serviços de computação em nuvem,
- tenham conexões lógicas (links) com a empresa ou
- qualquer outros que a área de *Compliance* julgue que por qualquer motivo possa gerar risco de cibersegurança à Gestora, previamente à sua contratação, na forma do Anexo II a esta Política.

O resultado será encaminhado ao Comitê de Segurança Cibernética para avaliação da

capacidade deles de evitar ataques cibernéticos e da potencial contratação, devendo a decisão sobre a contratação ficar formalizada, sendo periodicamente reavaliada.

1.16.2. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO NOS CONTRATOS COM TERCEIROS

A empresa deverá incluir em contratos com Colaboradores externos requisitos de segurança da informação nos contratos de prestação de serviços, bem como verificar a efetividade dos controles implementados pela empresa contratada para atender aos requisitos durante a vigência do contrato, na forma menciona acima.

Nesse sentido, a empresa investirá continuamente em ferramentas robustas para monitoramento do ambiente, como também na manutenção de equipe especializada com expertise na área

Para garantir as regras mencionadas nessa Política, a empresa deverá:

- Implantar sistemas de monitoramento nos servidores, correio eletrônico. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Para os riscos associados a pharming, phishing, vishing e smishing, conduzir treinamentos e campanhas periódicas, bem como testes pelo menos anualmente;
- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware se mantido servidor físico;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e
- Testar a vulnerabilidade e penetração do Website da Gestora, bem como
- de todo e qualquer sistema eletrônico desenvolvido internamente pela Gestora, ao menos semestralmente.

Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Gestora poderão ser acessados, caso o Comitê de Segurança Cibernética julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

1.17. Plano de Resposta a Incidente

A empresa deverá levar em consideração o plano de resposta a incidentes previstos que deve estar previsto no seu Plano de Continuidade de Negócios, considerando os cenários de ameaças (que inclui falha de segurança cibernética grave) e os descritos abaixo para os demais casos:

- Os Colaboradores poderão reportar incidentes diretamente ao Responsável pela TI.

1.17.1. PROCEDIMENTO EM CASO DE INCIDENTE

Uma vez que o Responsável pela Segurança da Informação (TI) tenha sido acionado devido a um potencial incidente, este deverá convocar o Comitê de Privacidade para que este delibere sobre a matéria.

1.17.2. AVALIAÇÃO INICIAL

Nessa etapa inicial, aspectos e decisões fundamentais deverão analisadas pela TI, pelo Comite de Privacidade e pela Diretoria e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

1.17.3. INCIDENTE CARACTERIZADO

Se for caracterizado um incidente, devem os membros do Comitê tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, informar à ANPD ou mais alguma autoridade, (ii) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa; e (iv) houve prejuízo para a empresa, se houve vazamento de dados e em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de segurança da informação, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor a desviar linhas de dados/e-mail.

1.17.4. RECUPERAÇÃO

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um *call* diário ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos. Também deverá se avaliar o impacto do incidente nos diversos riscos e caso necessário tomar as devidas ações, tais como manifestação pública na mídia, com eventual contração de assessor de imprensa.

Verificar se todas as informações necessárias estão seguras e a Diretoria definirá se outras medidas são necessárias. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da empresa, devem ser comunicados ao TI e a Diretoria e

consultor externo se houver.

1.17.5. RETOMADA

Esta fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a normalidade e, como será feita a reconstrução de sistemas e eventuais mudanças e medidas de prevenção. A Área de TI deverá registrar o histórico em local adequado, como o sistema de gerenciamento.

1.18. RECICLAGEM E REVISÃO

A empresa deverá manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização em cibersegurança com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades por meio de um Programa de Treinamento da empresa.

O Responsável pela Segurança Cibernética, em conjunto com DPO e o Comitê de Privacidade realizará a revisão e atualização desta Política periodicamente, no mínimo anualmente ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada.

FICHA TÉCNICA

Versão do documento: 01

Data de aprovação Da Política:27/11/2023

ANEXO I

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Nome_____, inscrito no CPF/MF sob o nº__, inscrito no RG _____ doravante denominado colaborador, e a Alibra Ingredientes SA, inscrita no CNPJ/MF sob o no. 03.645.657/0001-02 resolvem, para fim de preservação de informações pessoais e profissionais dos clientes e da EMPRESA, celebrar o presente Termo de Responsabilidade e Confidencialidade, que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais para os fins deste Termo:

a) Todo tipo de informação escrita, verbal podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias empresariais ou comerciais, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da empresa e a seus sócios ou clientes, independente destas informações estarem contidas em pen-drives, hard-drives, outros tipos de mídia ou em documentos físicos.

b) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na empresa, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da empresa e/ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela empresa ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

1.1 Não são consideradas Informações Confidenciais, quaisquer informações que: (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador; (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao disposto neste Termo; (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade; (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade; (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente ao RH ou à Diretoria imediata da empresa para que as medidas legais cabíveis sejam tomadas.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na empresa, comprometendo-se, portanto, observadas as disposições das Políticas da EMPRESA, a não divulgar tais Informações Confidenciais para quaisquer fins ou

pessoas estranhas à empresa, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1 O Colaborador se obriga a, durante a vigência deste Termo de Confidencialidade e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na empresa.

2.2 As obrigações ora assumidas ainda persistirão no caso do Colaborador ser transferido para qualquer subsidiária ou empresa coligada, afiliada, ou controlada pela Alibra Ingredientes AS.

2.3 A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita a apuração de responsabilidades nas esferas cível e criminal.

3 O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis para a empresa e terceiros, ficando desde já o Colaborador obrigado a indenizar a empresa, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1 O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, e demissão por justa causa do Colaborador, sem prejuízo do direito da empresa de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

3.2 O Colaborador expressamente autoriza a empresa a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou outros observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízo do direito da empresa exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.

3.3 A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados acima.

3.4 O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na empresa

são e permanecerão sendo propriedade exclusiva da EMPRESA e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na empresa, devendo todos os documentos permanecer em poder e sob a custódia da empresa, salvo se em virtude de interesses da empresa for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da empresa.;

b) Em caso de rescisão do contrato individual de trabalho, desligamento do Colaborador, este deverá restituir imediatamente à empresa todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da EMPRESA, sendo proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

d) É expressamente proibida a instalação pelo Colaborador, de softwares não homologados pela empresa nos equipamentos utilizados pelo Colaborador para desenvolver suas atividades profissionais.

e) A senha para acesso à rede de dados é pessoal e intransferível e não deverá, em nenhuma hipótese, ser revelada a outra pessoa.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a empresa, permitindo que esta procure a medida judicial cabível para atender ou evitar a revelação.

6. Este Termo é parte integrante das regras que regem a relação de trabalho do Colaborador com a empresa, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

6.1 A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas conforme descrito no Código de Ética ou em políticas da empresa.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 vias de igual teor e forma.

Cidade,_____de_____de 20____.

_____

NOME DO COLABORADOR OU EMPREGADO