DEZEMBRO DE 2021

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

ORIENTAÇÕES GERAIS E PROCESSOS

SOUZAMAAS ASSESSORIA EMPRESARIAL LTDA
13.651.988/0001-09

Sumário

1. INTRODUÇÃO

A **SOUZAMAAS** zela por relações transparentes e éticas e proíbe a prática de toda forma de corrupção, fraude, suborno, favorecimento e extorsão por seus colaboradores.

O objetivo deste documento é estabelecer as regras e orientações bases para a utilização segura e ética dos recursos tecnológicos da **SOUZAMAAS**, seguindo as normativas da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), visando a proteção dos dados pessoais de sua base de clientes, colaboradores e demais envolvidos.

A política aqui estabelecida deve ser cumprida por todas as partes envolvidas nas atividades vinculadas a **SOUZAMAAS**. É um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a todos os seus colaboradores e parceiros que venham ter acesso a dados pessoais e/ou recursos tecnológicos da **SOUZAMAAS**.

2. CONCEITOS BÁSICOS

Para efeitos de entendimento e fácil compreensão da política ora criada neste instrumento, serão apresentados as definições legais e conceitos que serão utilizados no decorrer deste documento;

a. **Dados:** Parte elementar da estrutura do conhecimento incapaz de, por si só, gerar conclusões inteligíveis ao destinatário, mas computáveis. Representa uma ação não descrita, uma quantidade sem especificar o objeto, por exemplo, dentro da LGPD temos os seguintes tipos de categorização de dados:
b. **Dados pessoais:** São todos os tipos de dados que podem levar a identificação de uma pessoa, de forma direta ou indireta. Alguns tipos de dados pessoais incluem (nome completo, RG e CPF, passaporte e carteira de habilitação, endereço, telefone, e-mail, endereço de IP, data de nascimento, localização via GPS, entre outros).
c. **Dados sensíveis:** Qualquer informação que relacione com a origem racial, étnica, credo, opinião política, filiação a sindicato; que se referem à saúde ou vida sexual, dados genéticos e biométricos
d. **Dados anonimizados:** Operação que seja realizada com os dados pessoais de forma anônima, sem que haja identificação do indivíduo
e. **Dados públicos:** São dados que ainda públicos podem ser restringidos pelo indivíduo.
f. **ANPD – Autoridade nacional de proteção de dados:** Órgão da administração pública direta federal com atribuições relacionadas a regulamentação e fiscalização do cumprimento da LGPD
g. **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
h. **Controlador:** Pessoa natural ou jurídica, a quem competem as decisões referentes ao tratamento de dados pessoais
i. **Operador:** Pessoa natural ou jurídica, que realiza o tratamento de dados pessoais em nome do controlador
j. **Encarregado de dados:** Responsável frente à ANPD e aos titulares indicados pelo controlador.

k. **Tratamento de dados**: Qualquer operação que seja realizada com os dados pessoais (incluindo: acesso, armazenamento, arquivamento, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização.

l. **Cliente:** Pessoa natural ou jurídica que contrate os serviços da **SOUZAMAAS**, ou que estejam em vias de contratar serviços.

m. **Colaborador:** Pessoa natural que faz parte do quadro de contratados e societário da **SOUZAMAAS**,

n. **Parceiro/Prestador**: Pessoa natural ou jurídica que prestas serviços a **SOUZAMAAS** no âmbito das atividades

o. **Recursos tecnológicos:** São todos os recursos físicos e digitais utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar informações. Entre os tipos de recursos podemos destacar: computares de mesa ou portáteis, smartphones, tablets, pen drive, discos externos, mídias, impressoras, scanner, entre outros

p. **Dispositivo móvel:** Entende-se qualquer equipamento eletrônico com atribuições de mobilidade, como: notebooks, smartphones e tablets.

q. **Incidentes de segurança da informação:** Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à esta política, a LGPD, falha de controles, ou situação previamente desconhecida, que possa ser relevante à segurança da informação. São exemplos de Incidentes de Segurança da Informação:
    i. Perda de serviços ou recurso;
    ii. Mau funcionamento ou sobrecarga de sistema;
    iii. Erros humanos;
    iv. Não conformidade com a Política e a Norma;
    v. Observações ou suspeitas de fragilidade em sistemas ou serviços;
    vi. Vazamento de informação de clientes ou pessoas físicas que estejam armazenadas e tratadas em nosso ambiente digital;
    vii. Violações de procedimentos de segurança e violações de acesso.

r. **LGPD – Lei geral de proteção de dados pessoais:** Lei de nº 13.709/2018 que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

s. **Criptografia:** é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

3. SEGURANÇA DA INFORMAÇÂO

Nos tópicos a seguir serão definidos normas, procedimentos e boas práticas de segurança da informação da **SOUZAMAAS**

3.1. REGRAS DE SEGURANÇA DA INFORMAÇÃO

Todas as informações geradas, acessadas, manuseadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas pelos colaboradores e parceiros, são de propriedade e direito de uso exclusivo da **SOUZAMAAS**.

Os colaboradores e parceiros devem zelar para que as informações inseridas nos sistemas, ou quando enviadas ao cliente, sejam livres de erro, transparentes e verídicas.

O acesso e uso das informações da **SOUZAMAAS**, incluindo o e-mail, devem estar limitados à jornada de trabalho ou período contratual do colaborador, exceto quando exercer atividade justificada ou plantões específicos devidamente controlados.

Todo e qualquer documento correspondente, bem como produzidas pela **SOUZAMAAS**, não poderão sair da empresa sem que seja por meio de protocolo de envio de documentos.

Quando necessária troca de informações com os clientes para cumprimento legal de obrigações, é necessário utilizar os canais oficiais disponibilizados pela empresa. Qualquer canal distinto ao correio eletrônico (e-mail), mensageiro eletrônico e sistema de arquivos oferecidos pela **SOUZAMAAS** é considerado um descumprimento das regras de segurança da informação e serão tomadas as medidas cabíveis quanto ao fato.

3.2. CONCESSÃO, REVOGAÇÃO E REVISÃO

A concessão de acesso aos recursos tecnológicos da **SOUZAMAAS** deve estar atrelada aos perfis de acesso previamente atribuídos ao colaborador em razão da sua atividade profissional exercida.

A solicitação de acesso deve ser realizada pelo gestor do colaborador ao responsável de tecnologia via sistema de chamados com todas as informações do usuário cadastrado.

O responsável de tecnologia se reserva ao direito de revalidar as permissões, ou não, caso a concessão tenha mais permissões do que o definido em política interna para a efetiva concessão.

Todos os acessos concedidos serão revisados, no mínimo, a cada 6 (seis) meses, a fim de garantir que continuam ativos e atualizados.

A revogação de acesso deve ocorrer mediante solicitação do gestor responsável pelo colaborador ou parceiro ao responsável de tecnologia. No entanto, os direitos de acesso podem

ser alterados e/ou revogados a qualquer tempo pela **SOUZAMAAS**, sem a necessidade de aviso prévio.

O acesso aos recursos tecnológicos será revogado imediatamente em caso de encerramento das atividades entre a **SOUZAMAAS** e as partes envolvidas. Portanto, assim que algum colaborador for demitido ou solicitar demissão, um parceiro tiver o contrato encerrado ou expirado, o responsável de TI tomará as providências necessárias.

3.3. USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

O colaborador deve utilizar apenas softwares e hardwares previamente homologados ou autorizados pelo responsável de tecnologia da **SOUZAMAAS**.

A gestão (instalação, manutenção e configuração) de todos os recursos tecnológicos é de responsabilidade exclusiva do responsável de tecnologia da **SOUZAMAAS**.

Todo colaborador ou parceiro que se distanciar de sua estação de trabalho ou do dispositivo móvel, deve imediatamente realizar o processo de bloqueio do equipamento.

Os equipamentos disponibilizados aos colaboradores e parceiros são de propriedade da **SOUZAMAAS**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da organização, bem como cumprir as recomendações e normas mencionadas neste documento.

As estações de trabalho e servidores contêm softwares de antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o responsável de TI.

Documentos imprescindíveis para as atividades dos colaboradores da organização deverão ser salvos em drives de rede. Tais arquivos não podem ser gravados apenas localmente nos computadores (por exemplo, no drive C:/), pois não terão garantia de backup (recuperação) e poderão ser perdidos caso ocorra uma falha no computador. Caso isso ocorra, a responsabilidade pela perda dos arquivos será do próprio usuário.

Os colaboradores devem informar ao responsável de TI qualquer identificação de dispositivo estranho conectado ao seu computador.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução ou auxílio do responsável de TI.

3.4. PERMISSÕES DIFERENCIADAS

Alguns cargos, de acordo com a definição de alçadas, cargos ou funções, podem ter permissões diferenciadas para o acesso e uso dos recursos tecnológicos, a fim de atender aos objetivos de negócio da **SOUZAMAAS**.

Excepcionalmente, podem ser concedidas autorizações adicionais, temporárias ou não, aos demais colaboradores, desde que tal solicitação seja aprovada, justificada e necessária para a execução de determinadas tarefas ou projetos.

3.5. VEDAÇÕES

Quando da utilização dos recursos tecnológicos da **SOUZAMAAS**, o colaborador ou parceiro não deve:

a. Realizar qualquer tipo de manutenção ou reparo nos recursos tecnológicos corporativos, exceto o responsável de tecnologia ou terceiro autorizado pela **SOUZAMAAS**;
b. Utilizar programas que burlem os controles de segurança e controle impostos pela **SOUZAMAAS** ou por seus normativos;
c. Executar programas de compartilhamento de arquivos ou estrutura diversa que permita a interconexão entre usuários de diversas localidades por meio de redes públicas, exceto quando prévia e expressamente autorizado;
d. Acessos de site que realizem o redirecionamento de tráfego (proxy) e burlem as políticas digitais;
e. Desinstalar ou desabilitar softwares instalados nos recursos tecnológicos pela **SOUZAMAAS** ou por alguém à sua ordem, independentemente do motivo;
f. Burlar quaisquer sistemas de segurança;
g. Acessar informações confidenciais sem explícita autorização do responsável;
h. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes;
i. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
j. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
k. Hospedar, acessar e compartilhar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país.
l. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.
m. Realizar a transferência e/ou a divulgação de qualquer software, programa ou dados para terceiros, por qualquer meio de comunicação (físico ou digital), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.
n. Armazenar arquivos pessoais e/ou não pertinentes ao negócio da **SOUZAMAAS** (fotos, músicas, vídeos etc.) para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores e acumular dados pessoais não necessário as

atividades da **SOUZAMAAS**. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, facultando a empresa em comunicar previamente o usuário.

o. A utilização de dispositivos removíveis de armazenamento de informações (pen drives, CDs, DVDs, HD Externos) para o transporte de informações. Em extremas necessidades e exceções é necessário acionar o responsável de TI para a avaliação do caso junto ao gestor responsável, se permitido, o dispositivo deverá conter tecnologia de criptografia. Todo o conteúdo transportado deve ser armazenado na rede corporativa e apagado do dispositivo imediatamente após a utilização
p. O consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
q. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato).
r. O acesso, armazenamento, utilização ou compartilhamento à conteúdo:
    i. agressivo, ofensivo, difamatório, ridicularizante, calunioso, constrangedor, violento, abusivo, homofóbico, racista ou político;
    ii. Que represente uma quebra de confidencialidade das informações da **SOUZAMAAS** ou de seus clientes;
    iii. Caracterize assédio moral ou sexual, ou que incitem a prática de crimes ou contravenções penais;
    iv. Constitua violação aos direitos de propriedade intelectual ou industrial da **SOUZAMAAS**, a exemplo dos bancos de dados, segredos de negócio, dados contábeis ou financeiros, ou de terceiros, incluindo a proteção de suas marcas e patente;
    v. Que denote ou estimule a perseguição preconceituosa baseada em cor, sexo, raça, incapacidade física ou mental, condição social, origem, religião ou outras situações protegidas pelas leis brasileiras.

3.6. GESTÃO DE INFORMAÇÕES

Todas as informações sigilosas, sejam elas físicas ou digitais, independente do formato ou local de armazenamento, da **SOUZAMAAS** ou de seus clientes, devem ser classificadas e rotuladas de forma a permitir fácil identificação e o tratamento adequado, ou seja, deve ficar claro quem pode ter acesso a ela e qual o nível de proteção que deve receber.

Informações confidenciais são aquelas que requerem tratamento especial, contendo conteúdo estratégico, contábil, financeiro, dados pessoais e críticos que, se divulgada, poderia violar a privacidade de indivíduos, revelar segredos de negócio dos nossos clientes, reduzir a vantagem competitiva da **SOUZAMAAS** ou causar impactos graves, sob o aspecto financeiro, legal, normativo, de reputação e de imagem aos nossos clientes.

O colaborador deve tratar como CONFIDENCIAL toda a informação que não estiver classificada, e comunicar ao gestor imediato, até que se defina ou se tenha conhecimento da sua classificação adequada.

O tratamento de informação classificada como CONFIDENCIAL deve atender os seguintes requisitos:

a. Estar rotulada como **SOUZAMAAS** em todas as páginas, além de identificar o colaborador, parceiros e/ou grupos autorizados para o acesso (físico e/ou digital);
b. Autorizar acesso apenas aos colaboradores e/ou parceiros previamente identificados;
c. Aplicar medidas de proteção lógica e física que garantam o acesso exclusivo pelos colaboradores e/ou parceiros autorizados;
d. Manter sigilo sobre o conteúdo ou informação para colaboradores e pessoas não autorizadas;
e. Por meios digitais, o compartilhamento deve ocorrer somente com autorização do gestor imediato e por meio dos recursos tecnológicos da **SOUZAMAAS**;
f. Em caso de compartilhamento de documentos por meio de dispositivos de armazenamentos móveis (pendrives, HDs externos, etc), a mídia deve conter aplicação de criptografia com nível de segurança compatível com o Advanced Encryption Standard (AES) ou superior;
g. Eliminar de maneira que impossibilite a posterior recuperação e o acesso à informação.

Somente é permitida a divulgação de qualquer informação da **SOUZAMAAS** ou de seus clientes, quando:

a. A divulgação é permitida expressamente por lei e autorização previa e por escrito pelo cliente e pela **SOUZAMAAS**;
b. A divulgação é exigida por lei, mas desde que seja autorizado previa e formalmente pela **SOUZAMAAS**;
c. Há o dever ou direito profissional de divulgação, mas desde que não proibido por lei e autorizado prévia e formalmente pela **SOUZAMAAS**.

No entanto, ao ser decido pela divulgação da informação, a **SOUZAMAAS** deve considerar:

a. Se os interesses de terceiros, incluindo partes cujos interesses podem ser afetados, podem ser prejudicados;
b. O tipo de comunicação que é esperado, a forma e mídia de divulgação, para quem deve ser dirigida; e se as partes para quem a comunicação é dirigida são as pessoas apropriadas para recebê-la.

A necessidade de sigilo profissional permanece mesmo após o término das relações profissionais entre a **SOUZAMAAS** e o colaborador. Assim, é proibido o uso ou compartilhamento de qualquer informação obtida, recebida ou gerada em decorrência do relacionamento profissional. Informação classificada como CONFIDENCIAL não deve ser publicada na Internet ou nas mídias sociais.

Não é permitido realizar o upload (transmitir arquivos) ou compartilhamento de informação, pessoais ou CONFIDENCIAIS, da **SOUZAMAAS** ou de seus clientes para serviços e aplicativos de comunicação instantânea, de armazenamento na nuvem ou repositórios digitais, a exemplo, mas não se limitando a Whatsapp, SnapChat, Viber, Facebook Messenger, Telegram, Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd, com exceção dos recursos tecnológicos disponibilizados e homologados pela **SOUZAMAAS**.

Informações confidenciais não devem ser discutidas, exibidas ou compartilhadas em ambientes públicos ou de livre acesso, onde pessoas alheias à **SOUZAMAAS** possam tomar conhecimento.

Antes do envio de informações confidenciais, independente se de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou outros meios, o colaborador deve confirmar a identidade e idoneidade do solicitante e a real necessidade do compartilhamento da informação solicitada. Em caso de dúvida, deve contatar o seu gestor imediato ou responsável de TI.

Informações confidenciais contidas em papéis, recursos tecnológicos e outras formas de suporte de dados não podem ficar expostas em mesas de trabalho, flipcharts, impressoras, fax, scanner, telas de computadores e nas salas de reunião, principalmente quando não estiverem sendo utilizadas.

3.7. GESTÃO DE IDENTIDADE

A identidade digital concedida ao colaborador é composta por um identificador único (ID ou nome do colaborador) e por um mecanismo de autenticação sigiloso (senha, biometria, token).

O responsável de tecnologia irá configurar o primeiro acesso do colaborador atribuindo uma senha temporária de modo que seja obrigatória sua a alteração em seguida da autenticação.

A senha deve ser tratada de forma individual, sigilosa e intransferível, não podendo ser compartilhada ou divulgada a terceiros. A senha não deve ser armazenada nos computadores ou dispositivos móveis, anotadas em papel ou em qualquer outro suporte físico ou eletrônico.

As senhas dos colaboradores devem:

a. Conter, pelo menos, 12 (doze) caracteres, dentre letras maiúsculas e minúsculas, números e símbolos,

   - 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;
   - Não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

b. Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 18 (dezoito) caracteres, dentre letras maiúsculas e minúsculas, números e símbolos;

   - Sempre que houver suporte à autenticação multifator (MFA) a mesma deve ser habilitada.

c. Serem trocadas entre 30 (trinta) e 120 (cento e vinte) dias, de acordo com direitos estabelecidos;

d. Não serem idênticas às últimas 5 (cinco) utilizadas.
e. Ser alteradas em qualquer caso de suspeita do comprometimento de seu sigilo ou vazamento.

Alguns dos sistemas utilizados pela **SOUZAMAAS**, por exemplo, o login de acesso as máquinas (Active Directory), respeitará a 3 (três) tentativas de acesso, sujeito ao bloqueio da conta do usuário. Para o desbloqueio é necessário que o usuário entre em contato com o responsável de TI. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

3.8. ACESSO À INTERNET

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, a **SOUZAMAAS**, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os colaboradores e parceiros devem estar sempre atentos ao uso da Internet e utilizar somente sites confiáveis e com o conteúdo relacionado às atividades da **SOUZAMAAS**.

Da mesma forma, todo colaborador ou parceiro deve ter extrema atenção quando do recebimento de arquivos executáveis, telas para acesso automático, solicitação de informações cadastrais na Internet, promoções exageradamente vantajosas, e outras atividades suspeitas de phishing.

Não é permitido obter e/ou conceder acesso não autorizado, monitorar, interceptar, desativar, sobrecarregar, obstruir ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de examinar ou testar vulnerabilidades em sistemas internos ou externos à **SOUZAMAAS**.

A **SOUZAMAAS** autoriza o uso moderado da Internet desde que não prejudique a atenção do colaborador durante a execução das suas atividades e a qualidade no desempenho de suas funções.

Não é permitida a utilização dos recursos tecnológicos da **SOUZAMAAS** com fins de entretenimento, como por exemplo, acesso a blogs, fotologs, salas de bate-papo, comunicadores instantâneos ou mídias sociais, exceto se liberado previa e expressamente pela **SOUZAMAAS**.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da organização, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privados da rede, visando assegurar o cumprimento de sua política.

A **SOUZAMAAS**, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades

decorrentes de processos civil e criminal, sendo que nesses casos a organização cooperará ativamente com as autoridades competentes.

É proibida a divulgação e/ou o compartilhamento indevido de informações em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores e parceiros não poderão utilizar os recursos da **SOUZAMAAS** para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores, neste caso, somente o responsável de TI tem permissão para acessar e utilizar programas de acesso remoto a outros computadores.

3.9. CORREIO ELETRÔNICO

O uso do correio eletrônico da **SOUZAMAAS** é para fins corporativos e relacionados às atividades do colaborador/parceiro dentro da organização.

Não é permitido o uso de correios eletrônicos particulares, a exemplo de Hotmail, Yahoo, Bol, Gmail, outros, para o envio e recebimento de informações da/sobre a **SOUZAMAAS** e seus clientes.

O colaborador deve utilizar adequadamente sua caixa postal corporativa, evitando que mensagens deixem de ser lidas ou fiquem sem resposta por mais de 24h (vinte e quatro horas) em dias úteis.

O colaborador deve organizar e efetuar a limpeza de sua caixa postal corporativa periodicamente, com o fim de evitar problemas de segurança e armazenamento, de modo a eliminar mensagens que, não tenham relação com o trabalho, ou que apresentem conteúdo suspeito que possam levar à eventual infecção da máquina por código malicioso.

O colaborador e parceiro devem verificar com atenção o endereço de correio eletrônico escolhido como destinatário para evitar o envio de mensagem para pessoa errada e que ocorra vazamento de informações da **SOUZAMAAS**, clientes e colaboradores. Contudo, se isso ocorrer, o colaborador deve tomar as seguintes providências:

a. Enviar imediatamente outra mensagem solicitando à pessoa que desconsidere a mensagem anterior e a exclua, pois aquele conteúdo não era destinado a ela.
b. Comunicar o encarregado de dados da **SOUZAMAAS**, relatando o ocorrido.

É vedado ao colaborador/parceiro:

a. Enviar mensagem eletrônica para um número indeterminado ou excessivo de destinatários, exceto quando autorizado e desde que esteja relacionado às atividades contratadas pela **SOUZAMAAS**;
b. Divulgar o endereço de e-mail corporativo para fins de recebimento de mensagens pessoais ou de entidades alheias aos interesses ou às atividades prestadas à **SOUZAMAAS**;

c. Falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
d. Apagar mensagens eletrônicas necessárias à **SOUZAMAAS**, sobretudo quando a **SOUZAMAAS** estiver sujeita a algum tipo de investigação, auditoria ou que possa ser prejudicada em procedimento judicial ou administrativo;
e. Encaminhar ou abrir mensagens consideradas suspeitas ou caracterizadas como corrente, SPAM e Phishing, sendo necessário a exclusão permanente (não deixar na lixeira);
f. Enviar mensagem com anexos contendo as seguintes extensões: .exe, .com, .bat, .pif, .js, .vbs, .hta, .scr, .cpl, .reg, .dll, .inf ou qualquer outro arquivo executável que represente um risco à segurança;
g. Veicular publicidade ou propaganda que caracterize concorrência desleal.
h. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
i. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou **SOUZAMAAS** ou suas unidades vulneráveis a ações civis ou criminais;
j. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
k. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da **SOUZAMAAS**;
l. Enviar mensagem que vise obter acesso não autorizado a outro computador, servidor ou rede;
m. Enviar mensagem que vise acessar informações confidenciais sem explícita e devida autorização;
n. Enviar mensagem que tenha conteúdo considerado impróprio, obsceno ou ilegal;
o. Enviar mensagem que seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
p. Enviar mensagem que contenham perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
q. Enviar mensagem que contenha fins políticos locais ou do país (propaganda política);

3.10. DISPOSITIVOS MÓVEIS E ACESSO REMOTO

Todo colaborador que fizer uso de dispositivos móveis disponibilizados pela **SOUZAMAAS**, ou particulares, quando autorizados prévia e expressamente para finalidades profissionais, deve atender as condições estabelecidas na presente política.

Os equipamentos são restritos aos colaboradores previamente autorizados, não sendo permitido o uso de dispositivos móveis disponibilizados pela **SOUZAMAAS** por outros colaboradores ou terceiros não-autorizados.

O colaborador deve devolver imediatamente e em perfeitas condições de uso e funcionamento o dispositivo móvel corporativo no caso de término de sua contratação à **SOUZAMAAS**, ou quando solicitado pela **SOUZAMAAS**, independentemente de qualquer motivo.

É vedado o uso de dispositivos móveis particulares para finalidades profissionais, exceto quando previamente autorizado.

Sobre o uso do dispositivo móvel, o colaborador ou parceiro deve, independentemente se a partir do dispositivo móvel corporativo ou particular autorizado:

a. Portar o dispositivo móvel sempre junto a si, ou trancado em ambiente seguro;
b. Informar imediatamente os casos de roubo, perda ou furto do dispositivo móvel, notificar imediatamente seu gestor direto e o responsável de TI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).
c. O colaborador deve armazenar nos dispositivos móveis corporativos somente arquivos relacionados às atividades profissionais no dispositivo móvel que estiver em posse;

Não é permitida a utilização de software sem a devida licença para realizar atividades profissionais ou produzir conteúdo para **SOUZAMAAS**.

Quaisquer danos eventualmente ocorridos no dispositivo móvel corporativo por má utilização do colaborador serão de sua responsabilidade, incluindo os custos decorrentes para a manutenção ou substituição do equipamento

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pelo responsável de tecnologia.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela organização constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É expressamente proibido a captura e divulgação de imagens pelos dispositivos móveis que contenham informações confidenciais, de clientes ou colaboradores.

3.11. HOME OFFICE

É expressamente proibido o uso de equipamentos particulares não autorizados pelo responsável de TI em conexões remotas ao ambiente da **SOUZAMAAS**. No caso de dispositivos habilitados e autorizados para acesso remoto, devem estar configurados pelo responsável de TI, obrigatoriamente, com mecanismos de segurança tais como sistema de criptografia, antivírus, ferramentas para acesso seguro à VPN (Virtual Private Network) e firewall pessoal, visando assegurar confidencialidade e a integridade das informações da **SOUZAMAAS**.

Os serviços remotos deverão ser interrompidos automaticamente após 5 (cinco) minutos de inatividade, porém, sempre que o colaborador/parceiro não estiver utilizando os recursos deve encerrar a sua sessão imediatamente.

3.12. BACKUPS

O responsável de TI criará as definições e executará os procedimentos e manuais operacionais específicos, conforme as características das informações, dos sistemas e das ferramentas de geração de backup, devendo considerar as seguintes diretrizes:

a. O armazenamento seguro e ambientalmente adequado em instalações locais e remotas das mídias, incluindo a eventual geração de backups redundantes como suporte às estratégias de contingência operacional e de continuidade de negócios;
b. Utilização de criptografia e restrição de acesso ao material salvaguardado;
c. O transporte seguro das mídias que terão armazenamento remoto;
d. O descarte seguro de mídias e ferramentas de geração de backups obsoletos, depreciados e danificados, considerando a eliminação definitiva de seu conteúdo e, quando necessário, a destruição do suporte físico.

4. PROTEÇÃO DE DADOS

Nos tópicos a seguir serão definidos normas, procedimentos e boas práticas de privacidade e proteção de dados, em especial os dados pessoais nos preâmbulos da LGPD.

4.1. TRATAMENTO DE DADOS E BASES LEGAIS

A **SOUZAMAAS** durante os processos e atividades diárias para o cumprimento dos objetos contratuais firmados com seus clientes e colabores inevitavelmente realiza o tratamento de dados pessoais de:

a. Colaboradores;
b. Parceiros;
c. Clientes

A **SOUZAMAAS** e todos seus colaboradores e parceiros durante todo o processo de tratamento de dados observará, em boa fé, todos os princípios e diretrizes da LGPD elencados no Art. 6º, da LGPD.

Este tratamento de dados pessoais, fica embasado em obrigações contratuais estabelecidas entre as partes, sejam elas obrigações de cunho comerciais ou administrativas, desta maneira, a **SOUZAMAAS** utiliza-se do art. 7º da LGPD com as seguintes hipóteses para realizar o tratamento de dados:

a. Para cumprimento de obrigação legal ou regulatória (Art. 7º, II, da LGPD);
b. Quando necessário para a execução de contrato ou de procedimentos preliminares a contrato do qual seja parte o titular de dados pessoais (Art. 7º, V, da LGPD),
c. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral (Art. 7º, VI, da LGPD);
d. Quando necessário para atender aos interesses legítimos do controlador ou de terceiros (Art. 7º, IX, da LGPD);

e. Para a proteção do crédito (Art. 7º, X, da LGPD).

Fica definida nesta política que a **SOUZAMAAS** como Controladora de dados pessoais de seus colaboradores, parceiros e clientes pode se utilizar de tratamento por terceiros, esses considerado pela LGPD como operadores. A **SOUZAMAAS** determina que estes operadores sigam as normativas da LGPD e suas boas práticas, garantido nível similar ao tratamento de dados que a **SOUZAMAAS** aplica, utilizando obrigatoriamente:

a. Uma política de privacidade e proteção de dados adequada as suas operações
b. Cláusulas contratuais referente a proteção de dados pessoais com seus colaboradores e fornecedores

Sobre a exclusão dos dados pessoais, ocorrerá mediante a solicitação dos titulares e será realizada somente nos casos que não houver nenhum impedimento legal ou necessidade de armazenamento a fim de garantir os direitos da **SOUZAMAAS**, conforme o Art. 16, I, da LGPD.

4.2. DIREITOS DO TITULAR

Os titulares de dados pessoais têm direito perante as informações armazenadas nas bases de dados da **SOUZAMAAS**, de acordo com o Art. 18 da LGPD a qualquer momento, requisitar a **SOUZAMAAS**, observando a proteção ao direito intelectual:

a. Confirmação da existência de tratamento;
b. Acesso aos dados;
c. Correção de dados incompletos, inexatos ou desatualizados;
d. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
e. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
f. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;
g. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
h. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
i. Revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

4.3. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os Incidentes de Segurança da Informação serão prevenidos:

a. Pela fiscalização do cumprimento da legislação vigente no Brasil, dos princípios éticos e dos controles estabelecidos pelos normativos da **SOUZAMAAS**;

b. Pelo monitoramento das vulnerabilidades existentes por meio de ferramentas de supervisão de atividades, registro e análise de trilhas de auditoria e controle de acesso em ambientes físicos e digitais.

O colaborador ou parceiro deve relatar todos os incidentes de segurança da informação que tiver conhecimento imediatamente para o encarregado de dados ou responsável de TI da **SOUZAMAAS**.

O colaborador não deve tomar qualquer ação própria em busca da solução do incidente de segurança da informação, devendo apenas relatá-lo.

Os incidentes de segurança da informação são quantificados e monitorados pelo responsável de TI e o encarregado de dados da **SOUZAMAAS**, a fim de se identificar quais podem ser mais recorrentes ou de maior impacto, além de permitir implementar ações corretivas e prevenir novas ocorrências.

Após notificação de um incidente de segurança da informação, o responsável de TI e o encarregado de dados da **SOUZAMAAS** tomam as ações necessárias para a mitigação de seus impactos e o restabelecimento da condição de normalidade, em seguida notificam a ANPD, se necessário, sobre o fato ocorrido.

As ações visam garantir a proteção aos direitos do titular de dados, a continuidade dos negócios da **SOUZAMAAS** e de suas atividades, além de realizar o isolamento do ambiente e do dispositivo, caso seja necessário.

Sempre que ocorrerem indícios do envolvimento de um colaborador ou parceiros em um incidente de segurança da informação, o responsável de TI ou encarregado de dados da **SOUZAMAAS** podem solicitar o bloqueio de sua identidade digital e demais acessos, além de informar imediatamente aos superiores.

As ações tomadas em resposta a um incidente de segurança da informação são armazenadas pela **SOUZAMAAS** de forma organizada e segura com a finalidade de compor uma base de conhecimento para a catalogação das experiências obtidas e análise da eficiência dos controles em vigor e possível auditorias dos órgãos responsáveis.

Em caso de constatação da possibilidade de haver processo jurídico o departamento jurídico será acionado imediatamente.

4.4. ARMAZENAMENTO E DESCARTE DE INFORMAÇÕES FÍSICAS

A **SOUZAMAAS** deve cumprir os diferentes prazos que a legislação estabelece para manutenção e guarda de documentos e livros fiscais, físicos e digitais, de acordo com a área correlata ao conteúdo das informações, a exemplo, mas não se limitando a documentos societários, tributários, trabalhistas e previdenciários.

Não é permitido o descarte em lixo comum de documentos confidenciais, como notas fiscais, fotocópias e cópias impressas. Os documentos dessa natureza devem ser triturados em seu descarte físico.

O responsável pela guarda de documentos deve manter o conteúdo organizado, em bom estado e de rápido acesso aos colaboradores e parceiros autorizados, sempre que necessário.

Da mesma forma, deve avaliar o estado físico da documentação, o volume a ser guardado e transferir toda documentação inativa ou não mais necessária para arquivo físico local ou terceirizado.

A guarda dos documentos deve ser organizada, sigilosa, segura (sem fonte de ignição para incêndio) e com movimentação restrita a colaboradores previamente autorizados.

4.5. TREINAMENTO

A **SOUZAMAAS** preza pela excelência da execução de suas atividades, sendo a segurança e proteção de dados uma delas, desta forma ela se compromete que seus colaboradores e parceiros passem por treinamento adequados e periódicos em boas práticas de segurança da informação de proteção de dados pessoais. Desta maneira fica determinada nesta política:

a. Treinamento anual de LGPD e Cyber Awareness
b. Treinamento LGPD e Cyber Awareness na integração de novos colaboradores e parceiros

Estes treinamentos são adotados como obrigatórios dentro da empresa, sempre serão ministrados por empresas ou profissionais capacitados com certificações que comprovem os conhecimentos sobre o assunto.

5. OUTRAS DISPOSIÇÕES

Nos parágrafos a seguir serão tratados políticas que abordam certos aspectos e requisitos da **SOUZAMAAS**

5.1. IDENTIFICAÇÃO VISUAL (CRACHÁ)

O uso do crachá de identificação **SOUZAMAAS** é obrigatório, pessoal e intransferível para todos os colaboradores. Deverá ser portado em lugar bem visível durante todo o tempo de permanência na empresa. Quando executar serviços externos, o colaborador também deverá usá-lo nas mesmas condições quando visitar os clientes. O uso do crachá é imprescindível para segurança do ambiente de trabalho.

Em caso de perda, um novo crachá deve ser requisitado imediatamente ao Departamento de RH.

5.2. CARTÃO DE ACESSO FISICO

A **SOUZAMAAS** disponibiliza aos seus colaboradores um cartão RFID para controle de acesso as suas dependências, este cartão é intransferível e de uso somente do portador, desta forma fica vedado o empréstimo dele a outro colaborador ou terceiro. O controle de acesso retem logs e é possível de auditoria se necessário.

5.3. CERTIFICADO DIGITAL

O único certificado digital a ser utilizado para execução das atividades laborais é o certificado e-CNPJ tipo A1 da **SOUZAMAAS**.

É vedado ao colaborador confiar a guarda ou compartilhar o certificado digital da **SOUZAMAAS** a terceiros, ou utilizar certificados digitais de terceiros sem a devida procuração.

É terminantemente proibido ao colaborador utilizar certificado digital de empresas-clientes, seja qual for a mídia (cartão, pen-drive, arquivo) ou nível de segurança (A1, A2, A3, A4).

É vedado ao colaborador utilizar seu certificado e-CPF, caso possua, para realizar trabalhos profissionais. Tal certificado deve ser mantido em sua posse.

Caso alguma das atividades exija a utilização do certificado digital do cliente/sócio e que não seja possível a utilização de procuração (por ex. e-CPF para entrega de declarações), deve exigir que o cliente compareça ao escritório em porte de seu certificado e acompanhe a tarefa a ser executada, solicitando que o mesmo digite sua senha quando da assinatura digital.

Quanto ao procedimento para outorgar e revogar procuração, o colaborador autorizado da **SOUZAMAAS** comparecerá no cliente e dará as devidas orientações para realizar as procurações, sendo elas: Receita Federal/Procuradoria Geral da Fazenda Nacional, Secretaria da Fazenda e Procuradoria Estadual, Caixa Econômica Federal/Conectividade Social.

Os dispositivos de identificação e senhas, incluindo os certificados digitais, protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a **SOUZAMAAS** e/ou terceiros. Por isso, o uso dos dispositivos, incluindo certificados digitais e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir uso compartilhado de identificação por mais de um colaborador, a responsabilidade perante a **SOUZAMAAS** e a legislação (cível e criminal) será dos usuários que dele se utilizarem

5.4. MONITORAÇÃO E INSPEÇÃO

Os colaboradores estão cientes de que a **SOUZAMAAS** realiza o registro e armazenamento de atividades (logs), e monitora todo acesso e uso de seus ambientes físicos e digitais com a captura de imagens, áudio ou vídeo, inclusive, com a finalidade de proteção de seu patrimônio e reputação e daqueles com quem se relaciona, de alguma forma, além de colaborar com as autoridades em caso de investigação.

Sempre que considerar necessário, a **SOUZAMAAS** pode auditar ou inspecionar os recursos de tecnologia que interagem com seus ambientes físicos ou digitais ou com suas informações, quando autorizada a entrada em suas dependências.

5.5. IMPRESSÃO

O serviço de Impressão destina-se exclusivamente a atividades de cunho empresarial da **SOUZAMAAS**. A sustentabilidade ambiental é elemento chave na utilização do serviço – a impressão de documentos deve ser evitada sempre que possível.

Deve-se buscar a tramitação de processos administrativos da **SOUZAMAAS** sempre na forma eletrônica, fazendo uso da impressão apenas nos casos em que se requer assinatura ou carimbos impressos ou que seja um pré-requisito.

Quando usado a impressão como apoio (por exemplo para conferência simultânea em tela) deve ser impressa em dupla-face sempre que possível. Evitar impressão de qualquer dado pessoal conforme informado elencado na LGPD

Ao imprimir qualquer documento o colaborador deverá adotar todos os cuidados de segurança necessários para que nenhuma pessoa sem autorização tenha acessa a dados confidenciais e/ou pessoais de qualquer cliente, colaborador e/ou fornecedor da **SOUZAMAAS**. Qualquer impresso que já cumpriu sua necessidade deve ser desfragmentado.

5.6. MESA LIMPA

A **SOUZAMAAS** adota as seguintes ações para minimizar os riscos associados ao acesso indevido, perda ou destruição de informações durante e fora de seu expediente:

a) Manter a sua mesa organizada;
b) Ao se ausentar da mesa, guardar qualquer documento que possa conter dados pessoais ou estratégicos da **SOUZAMAAS** e de seus clientes;
c) Não deixar exposto informações estratégicas, dados pessoais e senhas em postites ou papeis colados em sua mesa;
d) No final de expediente, recolher papeis e documentos da sua mesa, eliminando aqueles que não possuem mais uso.

Esta norma tem como objetivo definir ações que reduzam o risco de um incidente de segurança causado por documentos expostos nas instalações da **SOUZAMAAS** e de seus clientes.

6. PAPÉIS E RESPONSABILIDADES

Abaixo serão elencadas as responsabilidades dos envolvidos na política da segurança da informação e proteção de dados da **SOUZAMAAS**

Diretores, sócios e gestores

a. Aprovar os normativos da **SOUZAMAAS**;
b. Orientar e acompanhar o estabelecimento e a observância dos controles estabelecidos, além de analisar as questões específicas apresentadas pelos colaboradores da **SOUZAMAAS**.

Responsável de TI

a. Definir com as demais áreas da **SOUZAMAAS** os requisitos e controles adequados para a proteção das informações e recursos tecnológicos da **SOUZAMAAS**;
b. Avaliar periodicamente os sistemas e equipamentos, com o intuito de verificar o cumprimento dos normativos da **SOUZAMAAS**;
c. Implementar os controles de segurança previstos nesta norma para proteção das informações e dos recursos tecnológicos;
d. Manter os softwares de proteção instalados, ativos e atualizados;
e. Adquirir, de acordo com o orçamento da **SOUZAMAAS**, recursos tecnológicos quando autorizado pela Diretoria;
f. Tomar as medidas cabíveis em caso de perda, furto ou roubo de qualquer recurso tecnológico da **SOUZAMAAS**;
g. Proceder com a manutenção, instalação, análise, configuração ou remanejamento de quaisquer recursos tecnológicos da **SOUZAMAAS**;
h. Estabelecer mecanismos de identificação e autenticação de forma que possibilite a rastreabilidade das atividades do colaborador ou parceiro;
i. Fornecer a senha ao colaborador ou parceiro de forma segura, sigilosa e de maneira que a sua alteração seja exigida no primeiro acesso;
j. Auxiliar no processo de revisão de acessos concedidos;
k. Conceder, ajustar ou revogar o acesso do colaborador ou parceiro, quando solicitado formalmente ou em caso de encerramento das atividades;
l. Realizar e testar o backup das informações e recursos tecnológicos críticos para a **SOUZAMAAS**;
m. Realizar o monitoramento e manter o valor probatório dos registros para fins legais, preservando a confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações.

Responsável pelos Recursos Humanos

a. Auxiliar na promoção da divulgação e capacitação sobre segurança de informação na **SOUZAMAAS**;

b. Autorizar, ou não, a concessão de acesso solicitada pelo gestor do colaborador;
c. Comunicar formal e imediatamente qualquer admissão, alteração de cargo ou atividade dos colaboradores para o responsável de Tecnologia, para que este crie ou altere as contas de acesso correspondentes;
d. Realizar a revisão dos acessos concedidos, no mínimo a cada 6 (seis) meses, em conjunto com o responsável de TI;
e. Informar o encerramento das atividades, férias, licenças e ausência temporária dos colaboradores ao responsável de TI, imediatamente.

Responsável pelas Questões Jurídicas

a. Agir, sempre que acionado pelo pelos sócios e diretores, nos casos de incidente de segurança da informação que possam envolver processos jurídicos;
b. Elaborar uma tabela de temporalidade de modo a garantir o armazenamento e o descarte das informações de acordo com os prazos estabelecidos pela legislação nacional vigente.
c. Auxiliar nas adequações necessárias aos contratos de clientes, fornecedores e colaboradores

Gestor Responsável pelo colaborador / parceiro

a. Orientar constantemente suas equipes quanto ao uso ético, seguro e de acordo com a legislação nacional vigente dos ativos tangíveis e intangíveis da **SOUZAMAAS**;
b. Autorizar, ou não, o uso de dispositivos móveis corporativos ou particulares pelos colaboradores supervisionados;
c. Autorizar, ou não, a concessão de acesso remoto aos colaboradores supervisionados;
d. Assegurar o cumprimento desta Norma por parte dos colaboradores supervisionados;
e. Participar da investigação de incidentes de segurança relacionados às informações, Recursos de TIC e colaboradores sob sua responsabilidade.

Colaboradores e parceiros

a. Cumprir e manter-se atualizado com relação a esta Política;
b. Utilizar de forma ética, segura e de acordo com a legislação nacional vigente todos os ativos corporativos, respeitando os direitos e as permissões de uso concedidas pela **SOUZAMAAS**;
c. Zelar para que todas as informações inseridas nos recursos tecnológicos da **SOUZAMAAS**, ou quando enviadas ao cliente, sejam necessárias, livres de erro, transparentes e verídicas;
d. Utilizar as informações e os recursos tecnológicos da **SOUZAMAAS** somente para finalidades profissionais e restritas as atividades contratadas;
e. Classificar e rotular todas as informações confidenciais no momento da sua criação ou recebimento;
f. Tratar a senha de forma individual, sigilosa e intransferível, não compartilhando ou divulgando a terceiros;
g. Triturar as informações físicas, sempre que necessário o seu descarte;
h. Reportar imediata e formalmente qualquer caso comprovado, passível de comprovação ou cuja suspeita seja fundamentada de descumprimento desta política

ou de qualquer incidente de segurança da informação, sob pena de sua conduta ser considerada omissa, negligente ou conivente;

i. Atuar de forma transparente, evitando toda forma de corrupção, fraude, suborno, favorecimento, extorsão, benefícios e vantagens.

Encarregado de dados

a. Aceitar reclamações, comunicações e solicitações dos titulares de dados, prestar esclarecimentos e adotar providências;
b. Receber comunicações da autoridade nacional e adotar providências;
c. Orientar os colaboradores e os contratados da **SOUZAMAAS** a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
d. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares referente a LGPD
e. Está definido que a senhor Carlos Henrique Z. de Almeida responde como Encarregado de Dados da **SOUZAMAAS** e o e-mail para contato é o lgpd@souzamaas.com.br .

Comitê de Segurança e Privacidade de Dados

a. Aprovar e revisar anualmente, ou sempre que se faça necessário, o processo de gestão de riscos de tecnologia, de acordo com as boas práticas mundialmente reconhecidas.
b. Aprovar e revisar anualmente, ou sempre que se faça necessário, a política de segurança da informação, o processo de segurança da informação e o processo de gerenciamento de incidentes de segurança da informação em harmonia com as diretrizes nacionais, bem como as boas práticas de segurança da informação mundialmente reconhecidas.
c. Estabelecer no âmbito institucional uma cultura de boas práticas voltada para segurança da informação
d. Definir os serviços de tecnologia considerados críticos para o **SOUZAMAAS**;
e. Definir investimentos em segurança da informação, com base em relatórios de gestão de riscos e pesquisas de mercado.
f. Definir o apetite a risco de tecnologia da **SOUZAMAAS** em harmonia com as boas práticas de segurança da informação mundialmente reconhecidas.

7. PROCESSO DISCIPLINAR

O colaborador que tomar atitudes antiéticas, ilícitas, não autorizadas ou contrárias ao recomendado pela **SOUZAMAAS** devem ser consideradas violações por si só e estão sujeitas às sanções cabíveis, podendo variar desde advertência verbal ou escrita, até a rescisão do contrato por justa causa.

A tentativa de burla às diretrizes e controles estabelecidos pela **SOUZAMAAS** deve ser desestimulada e, quando constatada, será tratada como violação às normas da empresa.

Atos de desonestidade, incontinência de conduta ou mau procedimento, negociação habitual por conta própria ou alheia sem permissão, concorrência desleal, desídia, embriaguez habitual ou em serviço, violação de segredo da empresa, indisciplina ou insubordinação, abandono de emprego, lesão contra a honra ou boa fama de qualquer pessoa ou ofensas físicas nas mesmas condições e prática de jogos de azar, enquadrados no art. 482 da Consolidação das Leis do Trabalho – CLT, ao ocorrerem serão punidos com demissão por justa causa, obedecendo os preceitos legais.

No caso de parceiros que prestam serviços a **SOUZAMAAS**, terão as rescisões contratuais solicitadas de forma forçada por descumprimento da política ora mencionada.

8. DISPOSIÇÕES FINAIS

Esta política encontra-se disponível na pasta de rede e será enviada para todas as partes envolvidas nas atividades diárias da **SOUZAMAAS**, deverá estar disponível para os titulares de dados sempre que necessário, ou em caso de indisponibilidade, pode ser solicitada para o encarregado de dados da **SOUZAMAAS**.

Em caso de dúvidas, o colaborador ou parceiro pode solicitar os esclarecimentos necessários por meio do e-mail ao encarregado de dados da **SOUZAMAAS**.

Esta política deve ser revista e atualizada em intervalos não superiores a 2 (dois) anos, visando garantir que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente no Brasil.

São Paulo, 13 de dezembro de 2021.