POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E PRIVACIDADE DE DADO

O objetivo deste documento é estabelecer as regras e orientações para a utilização segura, ética e de acordo com a legislação vigente no Brasil dos Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC) e das informações da SOUZAMAAS.

APLICAÇÃO

Esta política é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a todos os seus colaboradores que venham a ter acesso e/ou utilizam as informações e/ou os Recursos de Tecnologia da Informação e Comunicação da SOUZAMAAS.

REGRAS DE SEGURANÇA DA INFORMAÇÃO

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.

Todas as informações geradas, acessadas, manuseadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade e direito de uso exclusivo da SOUZAMAAS.

Os colaboradores 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 às empresas clientes do escritório, bem como produzidas pela SOUZAMAAS, não poderão sair da empresa sem que seja por meio de protocolo de envio de documentos.

É proibido o envio de documentos impressos para os clientes em papel rascunho.

Cada setor tem sua classificação de documentos confidenciais. Esses documentos não podem ser reaproveitados (utilizados para rascunho). Devem ser destruídos imediatamente, por meio da fragmentadora.

Quando necessário troca de informações com os clientes para cumprimento legal de obrigações faz necessário utilizar os canais oficiais disponibilizados pela empresa, qualquer canal distinto ao correio eletrônico e sistema de arquivos oferecidos pela SOUZAMAAS é considerado uma não-conformidade e tomaremos as medidas cabíveis quanto ao fato.

RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Os Recursos de TIC da SOUZAMAAS, a exemplo do correio eletrônico, Internet, dispositivos móveis, acesso remoto e, são destinados para finalidades estritamente profissionais e restritas às atividades designadas para cada colaborador.

CONCESSÃO, REVOGAÇÃO E REVISÃO

A concessão de acesso aos Recursos de TIC e sistemas da SOUZAMAAS deve estar atrelada aos perfis de acesso previamente atribuídos ao colaborador em razão da sua atividade profissional exercida. Deve ser pontuado os seguintes tipos de acessos e permissões:

- Permissões de acesso as pastas na rede;
- Permissões de acesso a determinadas empresas nos sistemas (Contmatic e Dominio);
- Permissões a determinados grupos de e-mail.

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

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

O acesso aos Recursos de TIC e sistemas corporativos deve ocorrer somente por meios e equipamentos disponibilizados pela SOUZAMAAS.

A concessão de acesso para terceiros deve expirar em no máximo 90 (noventa) dias.

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 ao departamento 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 de TIC e sistemas corporativos serão revogados imediatamente em caso de encerramento das atividades entre a SOUZAMAAS e o colaborador.

USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

O colaborador deve utilizar apenas softwares e hardwares previamente homologados ou autorizados pelo departamento de TI da SOUZAMAAS.

A gestão (instalação, manutenção e configuração) de todos os Recursos de TIC corporativos é de responsabilidade exclusiva do departamento de TI.

Todos os Recursos de TIC corporativos contem softwares de proteção instalados, ativos e atualizados.

Todo colaborador que se distanciar do Recurso de TIC que estiver em uso, especialmente a sua estação de trabalho e o dispositivo móvel, deve imediatamente realizar o processo de bloqueio da estação.

Não é permitida a utilização de dispositivos removíveis de armazenamento de informações (pen drives, CDs, DVDs, HD Externos) para o transporte de informações, em caso de extremas necessidades e exceções é necessário acionar o departamento de ti para a avaliação do caso junto ao gestor responsável.

Todo o conteúdo transportado deve ser armazenado na rede corporativa e apagado do dispositivo imediatamente após a utilização

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 de TIC corporativos, a fim de atender aos objetivos de negócio da SOUZAMAAS.

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

VEDAÇÕES

Quando da utilização dos Recursos TIC da SOUZAMAAS, o colaborador não deve:

- Realizar qualquer tipo de manutenção ou reparo nos Recursos de TIC corporativos, exceto o departamento de TI ou terceiro autorizado pela SOUZAMAAS;
- Utilizar programas que burlem os controles de segurança e controle impostos pela SOUZAMAAS ou por seus normativos;
- Executar programas de compartilhamento de arquivos peer-to-peer (p2p) ou estrutura diversa que permita a interconexão entre usuários de diversas localidades por meio de redes públicas, exceto quando prévia e expressamente autorizado;
- Desinstalar ou desabilitar softwares instalados no Recurso de TIC pela SOUZAMAAS ou por alguém à sua ordem, independentemente do motivo;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- 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;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

Os equipamentos disponíveis aos colaboradores 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 constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É terminantemente proibida a conexão/utilização de pen-drives ou quaisquer outros dispositivos móveis que não pertençam a empresa.

Os sistemas e computadores contêm softwares de antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento de TI.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), 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.

Arquivos pessoais e/ou não pertinentes ao negócio da SOUZAMAAS (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, facultando a empresa em comunicar previamente o usuário.

Documentos imprescindíveis para as atividades dos colaboradores da organização deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:/, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da SOUZAMAAS e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do departamento de TI.

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

É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

Todos os recursos tecnológicos adquiridos pela SOUZAMAAS devem ter imediatamente suas senhas padrões (default) alteradas.

Quando da utilização de Recursos de TIC da SOUZAMAAS ou particular que estiver interagindo com seu ambiente lógico, o colaborador não deve acessar, armazenar, utilizar ou compartilhar qualquer conteúdo:

- Contrário à legislação vigente no Brasil, a moral, a ética ou as normas da SOUZAMAAS;
- Obsceno, sexual, pornográfico ou erótico;
- Agressivo, ofensivo, difamatório, ridicularizante, calunioso, constrangedor, violento, abusivo, homofóbico, racista ou político;
- Que represente uma quebra de confidencialidade das informações da SOUZAMAAS ou de seus clientes;
- Caracterize assédio moral ou sexual, ou que incitem a prática de crimes ou contravenções penais;
- 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;
- 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.

A SOUZAMAAS em zelo a sua marca, desde que não tenha autorização expressa do sócio administrador, é proibido sua utilização em qualquer meio de documento físico ou espaço digital (por ex. internet, redes sociais). A logomarca da empresa possui uma identidade visual para se comunicar com o mercado. Segue critérios rigorosos da sua história (criação), considerando formato, fonte e cores. Por isso, quanto expressamente autorizado deve seguir os padrões definidos.

CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações sigilosas, sejam elas físicas ou digitais, independente do formato ou local de armazenamento, da SOUZAMAAS ou se 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:

- Estar rotulada como CONFIDENCIAL em todas as páginas, além de identificar o colaborador, cliente e/ou grupos autorizados para o acesso (físico e/ou digital);
- Autorizar acesso apenas aos colaboradores e/ou clientes previamente identificados;

- Aplicar medidas de proteção lógica e física que garantam o acesso exclusivo pelos colaboradores e/ou clientes autorizados;
- Manter sigilo sobre o conteúdo ou informação para colaboradores e pessoas não autorizadas;
- O compartilhamento ou o transporte físico deve ocorrer mediante serviço postal ou mensageiro com serviço de entregas em mãos, por exemplo;
- Por meios digitais ou de telecomunicação, o compartilhamento deve ocorrer somente com autorização do gestor imediato e por meio da infraestrutura tecnológica da SOUZAMAAS;
- Em caso de compartilhamento digital externo, deve ocorrer a aplicação de criptografia ou cifragem com nível de segurança compatível com o Advanced Encryption Standard (AES);
- 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 divulgação é permitida expressamente por lei e autorização previa e por escrito pelo cliente e pela SOUZAMAAS;
- A divulgação é exigida por lei, mas desde que seja autorizado previa e formalmente pela SOUZAMAAS;
- Há o dever ou direito profissional de divulgação, mas desde que não proibido por lei e autorizado previa e formalmente pela SOUZAMAAS.

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

- Se os interesses de terceiros, incluindo partes cujos interesses podem ser afetados, podem ser prejudicados;
- Se todas as informações relevantes são conhecidas e comprovadas, na medida praticável. Quando a situação envolver fatos não comprovados, informações incompletas ou conclusões não comprovadas, a SOUZAMAAS deve usar o seu julgamento profissional para avaliar o tipo de divulgação que deve ser feita, caso seja feita;
- 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 CONFIDENCIAL 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.

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 departamento de tecnologia.

Informações confidenciais contidas em papéis, Recursos de TIC 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.

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 departamento de TI 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:

- Conter, pelo menos, 8 (oito) caracteres, dentre letras maiúsculas e minúsculas, números e símbolos;
- Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, dentre letras maiúsculas e minúsculas, números e símbolos;
- Serem trocadas entre 30 (trinta) e 120 (cento e vinte) dias, de acordo com direitos estabelecidos;
- Não serem idênticas às últimas 5 (cinco) utilizadas.

As senhas devem ser alteradas em qualquer caso de suspeita do comprometimento de seu sigilo.

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.

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 departamento de tecnologia da Informação. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, e são orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos serão imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o departamento de tecnologia da Informação tomará as providências necessárias.

QUANTO A 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.

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

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.

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).

Todos os dispositivos de identificação utilizados na SOUZAMAAS, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

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.

ACESSO À INTERNET

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a 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 devem estar sempre atentos ao uso da Internet e utilizar somente sites confiáveis, autorizados e com o conteúdo relacionado às atividades da SOUZAMAAS.

Da mesma forma, todo colaborador 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 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 de TIC 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.

Como é do interesse da SOUZAMAAS que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome da SOUZAMAAS para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

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.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pelo departamento de ti e computando também uma não conformidade pelo não segmento de nossas políticas.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da SOUZAMAAS para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

É proibido o download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato). Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload de qualquer software licenciado a SOUZAMAAS ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores 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.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos, bem como os serviços de comunicação instantânea, os quais serão bloqueados. Não é permitido acesso a sites de proxy.

CORREIO ELETRÔNICO

O uso do correio eletrônico da SOUZAMAAS é para fins corporativos e relacionados às atividades do colaborador/usuário 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 são mais necessárias para comprovação e documentação das atividades profissionais;
- Não configure registro para fins de comprovação da Política de Qualidade;
- Não tenham relação com o trabalho, ou que apresentem conteúdo suspeito que possam levar à eventual infecção da máquina por código malicioso.
- O colaborador deve 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:

- Enviar imediatamente outra mensagem solicitando à pessoa que desconsidere a mensagem anterior e a exclua, pois aquele conteúdo não era destinado a ela.
- Comunicar o departamento de ti e enviar um e-mail para lgpd@souzamaas.com.br relatando o ocorrido.

Todas as mensagens eletrônicas corporativas devem:

- Ter redação clara, objetiva e formal, além de estar livres de palavras ou expressões que possam caracterizar excesso de intimidade, tais como contato carinhoso, apelidos, uso de diminutivos ou termos que sejam inapropriados no ambiente de trabalho;

- Ser revisadas antes do envio, pois erros gramaticais, ortográficos ou de concordância devem ser evitados na SOUZAMAAS;
- As mensagens de correio eletrônica sempre deverão incluir assinatura no formato/imagem disponibilizada pela empresa.

As mensagens de correio eletrônica devem seguir fielmente o padrão abaixo:

- Assinatura do e-mail;
- O texto deve ser escrito em fonte Calibri, tamanho 11, na cor preta, é permitido alterar a cor de algumas palavras, sublinhá-la ou alterá-la para negrito quando necessário para destacar alguma parte do texto.
- Fundo do e-mail em cor branca;
- No campo Assunto é necessário seguir os padrões que consta no manual de qualidade e padronização.
- No campo Para conter as pessoas que estão destinadas o e-mail.
- No campo Cópia conter as pessoas que serão apenas informadas.

É vedado ao colaborador:

- Enviar mensagem eletrônica para um número indeterminado ou excessivo de destinatários, exceto quando autorizado e desde que esteja relacionado às atividades contratadas pela SOUZAMAAS;
- 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;
- Falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- 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;
- Encaminhar ou abrir mensagens consideradas suspeitas ou caracterizadas como corrente, SPAM e Phishing, sendo necessário a exclusão permanente (não deixar na lixeira);
- 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;
- Veicular publicidade ou propaganda que caracterize concorrência desleal.
- 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;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou SOUZAMAAS ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da SOUZAMAAS;

- Enviar mensagem que vise obter acesso não autorizado a outro computador, servidor ou rede;
- Enviar mensagem que vise acessar informações confidenciais sem explícita autorização do proprietário;
- Enviar mensagem que tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Enviar mensagem que seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Enviar mensagem que contenham perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Enviar mensagem que contenha fins políticos locais ou do país (propaganda política);

AUSÊNCIA DO COLABORADOR

Na ocorrência de férias, afastamento, licença ou ausência do colaborador, este deve:

- Inserir resposta automática de ausência temporária, divulgando endereço de e-mail e contato do colaborador responsável pelo recebimento das mensagens eletrônicas;
- Outorgar previamente uma procuração eletrônica para o colaborador responsável durante a sua ausência, caso utilize o certificado digital emitido em seu nome (e-CPF) para execução das atividades profissionais;
- Informar e indicar ao cliente o colaborador responsável durante a sua ausência, caso utilize sistema de comunicação específico.

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 deve, independente se a partir do dispositivo móvel corporativo ou particular autorizado:

- Portar o dispositivo móvel sempre junto a si, ou trancado em ambiente seguro;

- Informar imediatamente os casos de roubo, perda ou furto do dispositivo móvel.
- 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

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade, como: notebooks, smartphones e tablets.

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 departamento de TI

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

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 responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela SOUZAMAAS, notificar imediatamente seu gestor direto e o departamento de TI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

É expressamente proibido o uso de equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da SOUZAMAAS.

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

HOME OFFICE

É expressamente proibido o uso de equipamentos particulares não autorizados pelo departamento de ti em conexões remotas ao ambiente da SOUZAMAAS.

Os dispositivos habilitados e autorizados para acesso remoto devem estar configurados e serem os equipamentos próprios disponibilizados pela SOUZAMAAS, 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 não estiver utilizando os recursos deve encerrar a sua sessão imediatamente.

MONITORAMENTO 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 lógicos 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 TIC que interagem com seus ambientes físicos ou lógicos ou com suas informações, quando autorizada a entrada em suas dependências.

BACKUPS

O departamento de TI é responsável por definir e executar os procedimentos e manuais operacionais específicos, de acordo com as características das informações, dos sistemas e das ferramentas de geração de backup, de acordo com:

- 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;
- Utilização de criptografia e restrição de acesso ao material salvaguardado;
- O transporte seguro das mídias que terão armazenamento remoto;
- 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.

Periodicamente é realizados testes de restauração de dados pelo departamento de TI visando garantir a efetividade, eficiência e confiabilidade do procedimento.

RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os Incidentes de Segurança da Informação serão prevenidos:

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

O colaborador deve relatar todos os Incidentes de Segurança da Informação que tiver conhecimento imediatamente para o departamento de Compliance pelo e-mail lgpd@souzamaas.com.br.

O colaborador não deve tomar qualquer ação própria em busca da solução do Incidente de Segurança da Informação, devendo apenas relatá-lo, salvo em casos de prestação de socorro a uma vítima, quando possível fazê-lo, sem oferecer risco a si próprio ou ao socorrido.

São exemplos de Incidentes de Segurança da Informação:

- Perda de serviços ou recurso;
- Mau funcionamento ou sobrecarga de sistema;
- Erros humanos;
- Não conformidade com a Política e a Norma;
- Observações ou suspeitas de fragilidade em sistemas ou serviços;
- Vazamento de informação de clientes ou pessoas físicas que estejam armazenadas e tratadas em nosso ambiente digital;
- Violações de procedimentos de segurança e violações de acesso.

Os Incidentes de Segurança da Informação são quantificados e monitorados pelo departamento de Compliance, a fim de se identificar quais são 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 departamento de Compliance toma as ações necessárias para a mitigação de seus impactos (contorno) e o restabelecimento da condição de normalidade (resolução) e notificar a autoridade ANPD se necessário sobre o fato ocorrido.

As ações visam garantir 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 em um Incidente de Segurança da Informação, o departamento de Tecnologia ou Compliance 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 e armazenadas pelo 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.

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

Qualquer impresso que já cumpriu sua necessidade deve ser desfragmentado.

Informações sobre o número de páginas e título dos documentos, assim como data e hora da impressão, assim como o usuário responsável, são registradas e mantidas por tempo indeterminado;

O serviço de impressão é provido para uso da empresa, ele composto por uma ilha de impressão. Os equipamentos são contratados na forma de serviço e incluem manutenção de defeitos, fornecimento de tôner e outros suprimentos, descarte e reciclagem de partes e peças substituídas. Somente o papel deve será fornecido pela empresa. A manutenção das impressoras opera de modo proativo, substituindo insumos antes que gerem parada do serviço (por exemplo, troca de tôner).

Existe dois modelos de impressora com custos e capacidades diferenciados. Cada impressora tem um custo fixo por página, conforme seu modelo. Poderá existir uma franquia de impressão, que estabelece o quantitativo mínimo de impressões para viabilizar o planejamento financeiro dos serviços.

A SOUZAMAAS implementará um mecanismo de segurança, que habilita a impressão somente quando o usuário estiver perto da impressora.

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 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.

Para segurança das informações físicas e lógicas, a SOUZAMAAS contrata apólices de seguro compatíveis com seus riscos operacionais.

PAPÉIS E RESPONSABILIDADES

Diretoria, Sócios e Gestores

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

Responsável pela Tecnologia da Informação

- Definir com as demais áreas da SOUZAMAAS os requisitos e controles adequados para a proteção das informações e Recursos de TIC da SOUZAMAAS;
- Avaliar periodicamente os sistemas e equipamentos, com o intuito de verificar o cumprimento dos normativos da SOUZAMAAS;
- Implementar os controles de segurança previstos nesta Norma para proteção das informações e dos Recursos de TIC corporativos;
- Manter os softwares de proteção instalados, ativos e atualizados;
- Adquirir, de acordo com o orçamento da SOUZAMAAS, Recursos de TIC corporativos quando autorizado pela Diretoria;
- Tomar as medidas cabíveis em caso de perda, furto ou roubo de qualquer Recurso de TIC da SOUZAMAAS ou particular autorizado que esteja sendo usado para finalidade profissional;
- Proceder com a manutenção, instalação, análise, configuração ou remanejamento de quaisquer Recursos de TIC da SOUZAMAAS;
- Estabelecer mecanismos de identificação e autenticação de forma que possibilite a rastreabilidade das atividades do colaborador;
- Fornecer a senha ao colaborador de forma segura, sigilosa e de maneira que a sua alteração seja exigida no primeiro acesso;
- Auxiliar o setor de Compliance no processo de revisão de acessos concedidos;
- Conceder, ajustar ou revogar o acesso do colaborador, quando solicitado formalmente pelo setor de Compliance ou em caso de encerramento das atividades;

- Realizar e testar o backup das informações e Recursos de TIC críticos para a SOUZAMAAS, nos termos desta Norma;
- Realizar o monitoramento e manter o valor probatório dos registros para fins legais, preservando a confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações.

Responsável pelo setor de compliance

- Promover de forma eficaz a divulgação e a capacitação sobre segurança de informação na SOUZAMAAS, em conjunto com os diretores, sócios e gestores.
- Analisar e avaliar casos de violações e demais eventos negativos relativos à segurança da informação na SOUZAMAAS inclusive quando envolver a Internet e as Mídias Sociais, acionando a Diretoria ou outros responsáveis sempre que necessário;
- Analisar e identificar os riscos ligados aos Recursos de TIC, dados e informações gerenciadas para avaliar a necessidade de melhorias nos controles existentes;
- Autorizar, ou não, o uso de dispositivo móvel particular e o acesso remoto, sempre que solicitado pelo gestor do colaborador prévia e expressamente;
- Realizar testes para garantir a recuperação correta dos backups, sempre que necessário.
- Contratar, em conjunto com a Diretoria, apólices de seguros compatíveis com os riscos operacionais da SOUZAMAAS.

Responsável pelos Recursos Humanos

- Auxiliar o setor de Compliance na promoção da divulgação e capacitação sobre segurança de informação na SOUZAMAAS;
- Autorizar, ou não, a concessão de acesso solicitada pelo gestor do colaborador;
- Comunicar formal e imediatamente qualquer admissão, alteração de cargo ou atividade dos colaboradores para o departamento de Tecnologia, para que este crie ou altere as contas de acesso correspondentes;
- Realizar a revisão dos acessos concedidos, no mínimo a cada 6 (seis) meses, em conjunto com o Departamento de Tecnologia;
- Informar o encerramento das atividades, férias, licenças e ausência temporária dos colaboradores ao departamento de Tecnologia, imediatamente.

Responsável pelas Questões Jurídicas

- Agir, sempre que acionado pelo pelos sócios e diretores, nos casos de incidente de segurança da informação que possam envolver processos jurídicos;

- 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.
- Auxiliar nas adequações necessárias aos contratos de clientes, fornecedores e colaboradores

Gestor Responsável pelo Colaborador

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

Colaboradores

- Cumprir e manter-se atualizado com relação a esta Política;
- 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;
- Zelar para que todas as informações inseridas nos sistemas e Recursos de TIC da SOUZAMAAS, ou quando enviadas ao cliente, sejam necessárias, livres de erro, transparentes e verídicas;
- Utilizar as informações e os Recursos de TIC da SOUZAMAAS somente para finalidades profissionais e restritas as atividades contratadas;
- Classificar e rotular todas as informações confidenciais no momento da sua criação ou recebimento;
- Tratar a senha de forma individual, sigilosa e intransferível, não compartilhando ou divulgando a terceiros;
- Manter o certificado digital em local protegido e seguro, quando não estiver em uso, além de não utilizar certificado digital de qualquer terceiro;
- Triturar as informações físicas, sempre que necessário o seu descarte;
- Reportar imediata e formalmente qualquer caso comprovado, passível de comprovação ou cuja suspeita seja fundamentada de descumprimento desta Norma ou de qualquer Incidente de Segurança da Informação, sob pena de sua conduta ser considerada omissa, negligente ou conivente;
- Atuar de forma transparente, evitando toda forma de corrupção, fraude, suborno, favorecimento, extorsão, benefícios e vantagens.

Encarregado de dados

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

Comitê de Segurança e Privacidade de Dados

- Aprovar e revisar anualmente, ou sempre que se faça necessário, o processo de gestão de riscos de TIC, de acordo com as boas práticas mundialmente reconhecidas.
- 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.
- Estabelecer no âmbito institucional uma cultura de boas práticas voltada para segurança da informação
- Definir os serviços de TIC considerados críticos para o SOUZAMAAS;
- Definir investimentos em segurança da informação, com base em relatórios de gestão de riscos e pesquisas de mercado.
- Definir o apetite a risco de TIC da SOUZAMAAS em harmonia com as boas práticas de segurança da informação mundialmente reconhecidas.

PROCESSO DISCIPLINAR

O colaborador que tomar atitudes antiéticas, ilícitas, imorais, 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 artigo 482 da Consolidação das Leis do Trabalho – CLT, ao ocorrerem serão punidos com demissão por justa causa, obedecendo os preceitos legais.

DISPOSIÇÕES FINAIS

Esta política encontra-se disponível na pasta de rede S:/LGPD, ou em caso de indisponibilidade, pode ser solicitada para o departamento de Tecnologia.

Em caso de dúvidas, o colaborador pode solicitar os esclarecimentos necessários por meio do e- mail lgpd@souzamaas.com.br ou via sistema de chamados.

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.

Fica ressaltado que é proibido a publicação de rotinas de trabalho, processos, ramais, contatos, informações contábeis, pessoais de clientes, horários, trajetos e projetos nas mídias de qualquer natureza.

São Paulo, 13 de setembro de 2021.

ANEXO 1 - TERMOS E DEFINIÇÕES

Aplicativos de Comunicação: Conjunto de código e instruções compiladas, executadas ou interpretadas por um Recurso de TIC, hospedadas em um dispositivo ou na nuvem, que é usada para troca rápida de mensagens, conteúdos e informações multimídia.

Ativo Intangível: Todo elemento que possui valor para a SOUZAMAAS e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo da, mas não se limitando a, reputação, imagem, marca e notoriedade.

Autenticação: Etapa necessária para validar a identificação de qualquer colaborador que deseja acessar certa informação ou Recurso de TIC da SOUZAMAAS.

Autenticidade: Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

Certificado Digital: É a identidade digital da pessoa física e jurídica no meio eletrônico. Ele garante autenticidade, confidencialidade, integridade e não repúdio nas operações que são realizadas por meio dele, atribuindo validade jurídica.

Colaborador: Empregado, estagiário, prestador de serviço, terceirizado, representante, conveniado, credenciado, fornecedor, menor aprendiz, ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indiretamente, com a SOUZAMAAS.

Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.

Controle de Acesso: Poder destinado a conferir permissões e restrições ao acesso de dados, informações e Recursos de TIC da SOUZAMAAS aos seus colaboradores e de gerenciar as tarefas executadas por hardware, software e controles administrativos para monitorar a operação do sistema, com a finalidade de garantir a integridade dos dados, autenticando o colaborador, registrando os acessos e as alterações no sistema/informações.

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:

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).

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

Dados anonimizados: Operação que seja realizada com os dados pessoais de forma anônima, sem que haja identificação do indivíduo

Dados públicos: São dados que ainda públicos podem ser restringidos pelo indivíduo.

Disponibilidade: Garantia de que as informações e os Recursos de TIC estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

Dispositivos Móveis: Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido a sua portabilidade, como por exemplo, pen drive, celular, smartphone, computadores portáteis, tablet, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem, ou qualquer dispositivo que permita conexão à Internet (tais como dispositivos 3G e wi-fi), portabilidade ou armazenagem de dados.

Estação de Trabalho: Hardwares, incluindo periféricos, softwares da rede ou instalados no c:\, outlook e internet, bem como mesa, cadeira e armário.

Hardware: Parte física do equipamento, como por exemplo, circuitos de fios, placas, monitor, processadores, cabos, memória e disco rígido.

Identidade Digital: É a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política ou documentos de segurança da informação, falha de controles, ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

Informação: A informação é o conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Integridade: Garantia de que as informações estejam íntegras durante o seu ciclo de vida.

Internet: Rede mundial de computadores, na qual o usuário pode, a partir de um dispositivo, caso tenha acesso e autorização, obter informação de qualquer outro dispositivo que também esteja conectado à rede. O protocolo padrão utilizado na internet é o TCP/IP.

Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

Login: Identificação única dos usuários para acessarem sistemas computacionais ou recursos tecnológicos.

Recursos de Tecnologia de Informação e Comunicação (Recursos de TIC): São todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Entre os tipos de recursos podemos destacar: computares de mesa ou portáteis, smartphones, tablets, pen drive, discos externos, mídias, impressoras, scanner, entre outros. Sempre que mencionados de forma a não identificar seu possuidor ou proprietário, os Recursos de TIC compreenderão tanto os pertencentes à SOUZAMAAS quanto aos particulares em proveito corporativo. Caso contrário, haverá declinação de posse ou propriedade no próprio texto.

Repositórios Digitais (Cyberlockers): Plataformas de armazenamento na internet, a exemplo, mas não se limitando ao Google Drive, SkyDrive, Dropbox, iCloud, Box e SugarSync.

Risco: Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

Segurança da Informação: É a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

Software: Conjunto dos componentes que não fazem parte do equipamento físico propriamente dito e que incluem as instruções e programas, bem como os dados a eles associados, empregados durante a utilização do usuário.

Tecnologia de Nuvem: Método de fundação de sistema de informação baseado em interligação de dispositivos que gera um ambiente acessível por qualquer ponto de determinada rede, sem qualquer prejuízo de suas permissões ou qualidade de dados.

Violação: Qualquer atividade que desrespeite as diretrizes estabelecidas na Política ou em quaisquer dos demais documentos complementares.