maps registradora

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

VERSÃO 1.8

MARÇO 2025

MAPS Registradora
Política de Segurança da Informação
Histórico de Revisões

Versão	Data	Histórico
1.0	Junho 2018	Elaboração do documento.
1.1	Julho 2018	Atualização do documento.
1.2	Agosto 2020	Inclusão de informações relacionadas à LGPD.
1.3	Março 2021	Atualização e revisão do documento.
1.4	Julho 2021	Inclusão dos assuntos Mesa Limpa, Dispositivos Próprios e Móveis, Contatos com Autoridades, Imprensa e com Grupos Especiais.
1.5	Dezembro 2023	Inclusão do assunto “Obrigatoriedade de Utilização de Dispositivos Próprios no Exterior”
1.6	Março 2024	Alteração do assunto “7. Dispositivos Próprios e Móveis”
1.7	Fevereiro 2025	Inclusão do tema "Coleta e Monitoramento de Dispositivos (notebooks ou celulares corporativos)"
1.8	Março 2025	Alteração textual de "Grupo de Segurança da Informação" para "Comitê de Segurança da Informação".

As atualizações e aprovações desta política são registradas e monitoradas por sistemas de controles internos, garantindo sua integridade, versionamento, rastreabilidade e conformidade corporativa.

ÍNDICE

Definição

A MAPS Services S.A. (MAPS) considera a segurança e proteção de dados e informações como parte essencial de suas atividades e de sua responsabilidade social. A informação é um dos principais ativos da empresa, sendo assim o Comitê de Segurança da Informação da MAPS estabelece esta política, com os conceitos e diretrizes sobre segurança da informação, a serem observados por toda a empresa e parceiros, que visam proteger as informações da empresa, dos seus clientes, dos clientes dos seus clientes e de seus parceiros.

Objetivos

Estabelecer diretrizes que permitam a todos os colaboradores e parceiros da MAPS seguirem padrões de comportamento relacionados à Segurança da Informação, visando atender à proteção legal da empresa e do indivíduo. Tem como principais objetivos:

LEGALIDADE E JUSTIÇA

Os dados pessoais serão coletados e processados legal e corretamente em relação ao Titular dos dados, a fim de proteger os direitos individuais dos titulares dos dados.

CONFIDENCIALIDADE

Garante que a informação seja acessada somente por pessoas autorizadas, pelo período necessário.

DISPONIBILIDADE

Garante o acesso completo às pessoas autorizadas, sem demora.

INTEGRIDADE: DADOS PRECISOS E OPORTUNOS

Garante que a informação se mantenha íntegra em seu estado original, sem modificações acidentais ou propositais da informação ou de parte dela. Dados pessoais devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Devem ser adotadas medidas permanentes para garantir que dados imprecisos ou incompletos sejam excluídos, corrigidos, suplementados ou atualizados.

LIMITAÇÃO DE FINALIDADE

Garante que informações e dados sejam coletados apenas para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

TRANSPARÊNCIA

Garante que o titular dos dados seja informado sobre como seus dados são processados. Trata-se da garantia, aos Titulares, de informações claras, precisas e acessíveis sobre o tratamento e os agentes de tratamento, observados os segredos comercial e industrial.

REDUÇÃO E MINIMIZAÇÃO DE DADOS

Garante que as informações e dados pessoais processados serão apropriados, relevantes e limitados ao mínimo necessário. Sempre que a meta permitir e os custos envolvidos forem proporcionais ao objetivo, dados anônimos devem ser usados.

LIMITE DE ARMAZENAMENTO

Garante que informações e dados pessoais sejam retidos de uma forma que permita a identificação dos indivíduos envolvidos, exceto quando a anonimização se fizer necessária, pelo tempo que for necessário para cumprir a finalidade para a qual os dados são processados. Dados pessoais não serão retidos por período maior que o necessário.

DIREITOS DOS TITULARES DE DADOS

A MAPS respeita os direitos de todos os titulares de dados e trata seriamente qualquer solicitação de Dados Pessoais, permitindo que os indivíduos corrijam, excluam ou restrinjam o processamento de seus Dados Pessoais.

EXCLUSÃO DE DADOS PESSOAIS

Garante que a MAPS remova Dados Pessoais que não sejam mais necessários para os fins para os quais foram coletados, ou se o consentimento for retirado e nenhum outro propósito legítimo para o processamento de dados se aplicar.

SEGURANÇA DOS DADOS

Os Dados Pessoais são processados com segurança. Devem ser tomadas medidas técnicas e operacionais apropriadas em relação à segurança dos dados, processamento ou alteração não autorizada, perda ou destruição e contra divulgação não autorizada e acesso não autorizado aos dados pessoais transmitidos, armazenados ou processados.

NÃO DISCRIMINAÇÃO

A MAPS não promove a realização do tratamento de Dados Pessoais para fins discriminatórios ilícitos ou abusivos.

RESPONSABILIDADE NO PROCESSAMENTO DE DADOS PESSOAIS

A MAPS, na qualidade de Operadora ou Controladora, conforme a ocasião, será responsável pela conformidade com a LGPD e demonstrará a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Abrangência

As regras especificadas nesta Política de Segurança da Informação ou simplesmente "Política" são aplicáveis a todos os colaboradores da MAPS (funcionários, estagiários ou prestadores de serviço) e parceiros (parceiros e fornecedores) que tenham acesso aos recursos da empresa (rede, sistemas, dados).

Diretrizes

A. ASPECTOS GERAIS

As informações da MAPS, de seus clientes e parceiros devem ser tratadas sempre de forma ética e sigilosa. Os dados e os ambientes tecnológicos usados pelos colaboradores, mesmo aqueles produzidos pelo colaborador em seu ambiente de trabalho, são de propriedade da empresa, e não podem ser entendidos como de uso pessoal. Permite-se o uso dos recursos para uso pessoal, desde que sem prejuízo ao desempenho do profissional ou dos serviços tecnológicos da empresa (rede, servidores, banda de internet).

São consideradas informações cobertas por esta Política, quaisquer informações, especificações, modelos, documentos, análises, testes, projetos, estudos, materiais de marketing, esboços, programas de computador, dados sobre produtos, processos e serviços, material estratégico, comunicados escritos ou verbais, quaisquer informações não disponíveis ao público ou obtidas via comunicação escrita ou verbal, em papel ou formato eletrônico. Podem existir em diferentes formas, como em sistemas, banco de dados, material impresso, dispositivos eletrônicos, diretórios na rede, equipamentos portáteis e na comunicação oral.

O colaborador ou parceiro que receber informações desta natureza deve mantê-las sob sigilo, bem como limitar seu acesso, controlar cópias e evitar que sejam repassadas a terceiros. Além disso, deve ter ciência de que o uso da informação e do ambiente tecnológico da empresa é monitorado, e que os registros obtidos podem ser utilizados na detecção de violações e como evidência para as penalizações que podem ocorrer (medidas corretivas, processos administrativos e processos judiciais).

Cada área da MAPS deve documentar os procedimentos nos quais os dados pessoais são processados em um registro de atividades de processamento. Disposições estabelecidas pela MAPS para documentação (como ferramentas de software e instruções na documentação) devem ser observadas.

B. REQUISITOS DESTA POLÍTICA

Esta Política deve ser revisada e atualizada pelo Comitê de Segurança da Informação da MAPS, sempre que algo relevante demandar ou quando o Comitê julgar necessário.

Todos os colaboradores e parceiros devem ser informados sobre esta Política logo na fase de contratação. Eles devem se comprometer a agir conforme as diretrizes aqui estabelecidas, por meio da adesão formal ao Termo de Responsabilidade.

Deve constar de todos os contratos da MAPS com parceiros, fornecedores e clientes, Cláusula ou Anexo de Acordo de Confidencialidade, principalmente se estes tiverem acesso a alguma informação, disponibilizada pela empresa.

As informações devem ser classificadas de acordo com o grau de criticidade e confidencialidade, e devem ser atribuídas a um ou mais responsáveis que determinarão o grau de acesso que outros devem ter.

C. CONTROLE DE ACESSO A SISTEMAS E RECURSOS DE REDE

A identificação de qualquer pessoa com acesso aos recursos e informações da MAPS deve ser única, pessoal e intransferível. Cada indivíduo é totalmente responsável pela posse e utilização de suas senhas e autorizações de acesso a ele concedidas, sendo proibido compartilhá-las. Deve manter a confidencialidade de suas senhas, alterá-las sempre que houver suspeita de que possam estar comprometidas e bloquear seu equipamento quando se ausentar para que outros não o utilizem enquanto estiver conectado com sua identificação.

Os acessos devem ser concedidos seguindo o critério do menor privilégio, ou seja, cada usuário só deve ter acesso aos dados e recursos que são imprescindíveis para o desempenho de seu trabalho. Acessos desnecessários ou excessivos devem ser revogados.

Ambientes de produção devem ser totalmente segregados e controlados com extrema rigidez.

D. CORREIO ELETRÔNICO

O correio eletrônico (e-mail) da MAPS é para uso corporativo e relacionado às atividades do usuário dentro da empresa. É proibido aos usuários de e-mails da empresa:

» Enviar qualquer mensagem que possa trazer riscos à empresa de ações civis ou criminais, como mensagens com ameaças (vírus, *spam*, *trojans*); com conteúdo que contrarie os interesses da empresa, impróprio, obsceno ou ilegal; mensagens que busquem acessar dados confidenciais ou que busquem acesso não autorizado a algum recurso; mensagens que possam assediar o destinatário ou causar prejuízo a qualquer pessoa ou empresa; mensagens que incluam material protegido por direitos autorais (caso não haja autorização do detentor do direito); mensagens com fins políticos, de caráter preconceituoso, violento, ofensivo, ameaçador ou difamatório.

- Divulgar dados não autorizados sem consentimento do proprietário da informação;
- Apagar mensagens que possam expor a empresa a algum tipo de investigação.

Todo usuário de correio eletrônico da empresa deve usar a assinatura e formato definidos no Guia de E-mail da MAPS.

E. INTERNET

O uso da internet é ferramenta de grande valor para todos, e seu mau uso pode trazer impacto para a produtividade dos colaboradores e para a reputação da empresa. É proibido:

- Instalar *softwares* piratas;
- Invadir sites de terceiros;
- Acessar páginas com conteúdo pornográfico, em especial material de pedofilia;
- Navegar por sites que incitem a violência, o terrorismo, que façam apologia às drogas ou que tenham conteúdo preconceituoso, ofensivo, discriminatório;
- Compartilhar informações confidenciais da empresa ou de seus clientes e parceiros;
- Baixar e instalar programas de fontes de procedência duvidosa, ou executar atividades que possam trazer vírus, *trojans*, *worms* para a rede da empresa;
- Fazer uso, distribuição, instalação ou cópia não autorizada de material ou *softwares* protegidos por direitos autorais.

O acesso dos colaboradores à Internet da MAPS para fins pessoais é de responsabilidade exclusiva do usuário. Além disso, os colaboradores devem ter ciência que o uso da Internet ou dos equipamentos da MAPS para fins pessoais pode ser monitorado, e que os registros obtidos podem ser utilizados para detecção de violações da Política de Segurança da Informação.

F. NOTEBOOKS E SERVIDORES

Os equipamentos disponibilizados para os colaboradores são de propriedade da MAPS, sendo que cada um é responsável pelo correto uso e manuseio para atender as necessidades da empresa.

Os notebooks e servidores devem possuir *softwares* antivírus instalados e atualizados sempre (nos casos em que se aplicam). Caso haja suspeita de vírus ou problemas de ordem técnica, a equipe de Infraestrutura da empresa deve ser acionada.

Arquivos salvos pelo usuário localmente nas estações de trabalho não possuem *backup* e são de inteira responsabilidade do usuário. Os arquivos necessários para execução das atividades da empresa devem ser salvos pelos usuários em servidores na rede com *backup* regular, e guardados por serviços corporativos de guarda de arquivos.

Não é permitido qualquer manutenção física ou lógica, instalação ou configuração dos equipamentos sem prévio conhecimento da equipe de Infraestrutura da MAPS.

Se necessário, o colaborador pode levar seu notebook para casa ou até um cliente, e conectar a redes de banda larga destes locais reconhecidamente seguros, mas será responsável por zelar pelo equipamento, e seguir a Política de Segurança da Informação, ainda que conectado em redes de banda larga de terceiros. Em caso de furto ou roubo, o colaborador é responsável e deve procurar autoridades policiais para fazer um boletim de ocorrência (BO), além de comunicar imediatamente seu gestor.

G. GESTÃO DE VULNERABILIDADES

A MAPS reconhece a importância da gestão de vulnerabilidades como um tema essencial para a proteção de seus ativos de informação contra ameaças. Dessa forma, estabelece-se uma norma específica que orienta a empresa quanto à identificação, avaliação, tratamento e monitoramento de vulnerabilidades em seus sistemas, redes e aplicações.

H. COLETA E MONITORAMENTO DE DISPOSITIVOS (NOTEBOOKS OU CELULARES CORPORATIVOS)

O time de Operações da MAPS reserva-se o direito de recolher o notebook ou celular corporativos do colaborador, quando julgar necessário para manutenção, atualização, substituição, auditoria ou outras razões operacionais e de segurança. No caso de uso de celular o corporativo, o colaborador deve comprometer-se a utilizar o chip exclusivo fornecido pela empresa.

Os dispositivos não devem, sob nenhuma hipótese, serem utilizados para prática de atividades ilícitas em descumprimento da legislação vigente ou das políticas e procedimentos internos da MAPS, incluindo, mas não se limitando ao recebimento e/ou compartilhamento de pornografia infantil, exploração sexual, cometimento de fraudes, entre outros.

A MAPS poderá monitorar todo o conteúdo contido ou trafegado nos dispositivos ou trafegados em seus ambientes lógicos, a seu exclusivo critério, por todos os meios necessários e pode, a qualquer tempo, inspecionar tais dispositivos, inclusive por meio de sua coleta e inspeção remota ou fisicamente. Caso solicitado acesso aos dispositivos, o colaborador deve comprometer-se a disponibilizá-lo prontamente para que o time de operações possa acessá-lo, podendo inclusive obter cópia do conteúdo disponível nos mesmos, bem como comprometer-se a disponibilizar todas as senhas de acesso aos equipamentos e a todas suas funcionalidades relacionadas ao desempenho das atividades laborais (i.e., e-mails, mensagens de texto, aplicativos de mensagens, incluindo WhatsApp, entre outros).

O recolhimento será realizado com aviso prévio ao usuário responsável pelo equipamento, exceto em casos de urgência, como risco à segurança da informação, falhas críticas ou necessidade de intervenção imediata.

Os equipamentos recolhidos serão registrados e devolvidos em prazo a ser estipulado, de acordo com a complexidade da intervenção necessária. Durante este período, quando possível, será disponibilizado equipamento substituto para garantir a continuidade das atividades do colaborador.

Caso o colaborador não entregue o equipamento solicitado, tome atitudes ou aja em desacordo com o que esta política determina, estará sujeito às sanções administrativas e legais apropriadas.

I. DISPOSITIVOS PRÓPRIOS E MÓVEIS (BYOD)

Os dispositivos utilizados pelos colaboradores para com suas respectivas atividades laborais, podem ser provenientes da própria MAPS ou do próprio colaborador. Sobre o tema, fica estabelecido que:

- Os dispositivos móveis concedidos pela empresa (*Company-Provided Devices*) como: celular, modem 3G/4G, notebook, devem ser utilizados **OBRIGATORIAMENTE** e **EXCLUSIVAMENTE** para execução das atividades da MAPS;
- Caso colaborador deseje trabalhar com equipamento próprio (*Bring Your Own Device*, ou BYOD), poderá fazê-lo, nas seguintes condições:
  - More ou vá morar no exterior (mais detalhes sobre o tema no tópico “Obrigatoriedade de Utilização de Dispositivos Próprios no Exterior”);
  - Se não se enquadrar na condição descrita acima e quiser utilizar o equipamento próprio, o colaborador deverá seguir o procedimento de solicitação para utilizar equipamento próprio, descrito no portal de processos da MAPS.

- Em ambas as situações, tanto para dispositivos próprios quanto da empresa, o colaborador será submetido aos seguintes procedimentos do Time de Operações:
  - Instalação de softwares básicos de proteção, como antivírus ou EDR, VPN e software de gestão de ativos utilizado pela MAPS (não é permitida a remoção desses softwares sem a conscientização da área de Operações);
  - Os dispositivos devem ser protegidos por métodos de autenticação forte, como senhas complexas, biometria ou tokens, para garantir o acesso apenas a usuários autorizados;
  - Os dados corporativos devem ser mantidos separados dos dados pessoais nos dispositivos, utilizando-se de contas separadas ou tecnologias de virtualização, quando aplicável.

Para que não haja vazamento de informações, fica estabelecido que:

- A MAPS fornecerá treinamento regular sobre segurança da informação e conscientização sobre os riscos de vazamento de informações, incluindo práticas recomendadas para prevenção;
- Todos os colaboradores devem estar cientes e concordar com a política de uso aceitável, que estabelece as diretrizes para o uso responsável dos dispositivos pessoais no ambiente de trabalho;
- A MAPS implementará ferramentas de monitoramento para detectar atividades suspeitas ou comportamentos de risco nos dispositivos pessoais dos funcionários.

AVISO: O desvio desta conduta poderá acarretar sanções disciplinares ou administrativas. Para mais informações sobre as regras de uso de dispositivos, leia sobre o tema na Política de Segurança Cibernética.

Obrigatoriedade de Utilização de Dispositivos Próprios no Exterior

Caso o colaborador venha a realizar as suas atividades laborais fora do território nacional, seja de forma definitiva ou temporária (superior a 30 dias), o mesmo deverá obrigatoriamente utilizar equipamento próprio e devolver o equipamento da empresa. Além de seguir todas as regras descritas neste documento, caberá ao interessado avisar a área de Operações de TI com 30 dias de antecedência, para que seja checado se as configurações e desempenho da máquina são compatíveis com as demandas internas.

No local de prestação dos serviços fora do território nacional, é necessário garantir que haja um serviço de internet estável e velocidade suficiente para transferência de arquivos e participação em vídeo conferências, bem como identificar previamente um local para se dirigir, caso tenha queda de energia, por período superior a 2 horas.

O eventual custo de manutenção do equipamento será de inteira responsabilidade do colaborador, e porventura, as horas ou dias que ficar impossibilitado de realizar as suas atividades, em razão de quebra ou mal funcionamento do equipamento, falta de energia ou internet, serão debitadas do banco de horas. Neste caso, também é recomendável identificar previamente um local para locação temporária de equipamento.

Vale lembrar que o horário de trabalho deverá ter como referência o horário de Brasília, tendo em vista a interação com os demais membros da equipe. Para efeito de feriados, será considerado os que tinha na cidade de origem, antes da mudança.

J. MESA LIMPA

Cada colaborador é responsável pela segurança física do seu ambiente de trabalho. O computador só pode ser acessado mediante entrada de senha, que deve ser requisitada ao ligar e ao destravar a tela. O equipamento só pode estar destravado na presença do colaborador, que deve desligá-lo ou travar a tela ao se ausentar.

O uso de formas não eletrônicas, tais como: papéis, anotações, lembretes, qualquer outra forma não eletrônica de informação, além de mídias removíveis, deve ser evitado ao máximo, principalmente para informações restritas ou confidenciais.

Caso seja absolutamente necessário o uso desses meios físicos:

- Devem ser mantidos seguros quando não estiverem em uso.
- Não faça refeições, lanches ou mesmo deixe líquidos como água/café/suco sobre a mesa enquanto esses documentos estiverem sobre a mesma.
- Descarte seguro, de preferência com picotadora ou de forma que os dados não possam ser identificados.
- Documentos obtidos para consulta devem retornar ao local de armazenamento assim que for concluído o seu uso.

K. CONTATOS COM AUTORIDADES, IMPRENSA E COM GRUPOS ESPECIAIS

Contatos com autoridades e imprensa devem ser realizados exclusivamente por representantes legais da MAPS, tal como membros da direção ou com autorização formal destes.

São exemplos de autoridades:

- Órgãos governamentais.
- Imprensa em geral.

Grupos especiais são organizações ou associações de indivíduos externos à empresa, com os quais mantemos contato como parte do nosso trabalho.

São exemplos de grupos especiais:

- Consultorias.
- Órgãos reguladores.
- Agentes do mercado.
- Entidades de ensino.

Caso o colaborador tenha contato com grupos especiais no desempenho de suas funções, deve ser observado:

- Não compartilhamento de informações confidenciais da MAPS. Caso necessário deve haver Acordo de Confidencialidade entre as partes.
- Cuidado com a legitimidade da fonte e qualidade da informação fornecida.
- Postura profissional e ética.

Responsabilidades

Os papéis e respectivas responsabilidades dos envolvidos por esta política, são:

Comitê de Segurança de Informação da MAPS

- Representar o compromisso da Gestão da empresa com a Segurança da Informação;
- Planejar e tomar providências para implantação de medidas de segurança que atendam aos objetivos desta Política;
- Garantir a atribuição dos recursos necessários (financeiros, humanos e tecnológicos) para a implementação desta Política;
- Propor iniciativas relacionadas à melhoria da Segurança da Informação da empresa;
- Promover a divulgação da Política e conscientização sobre Segurança da Informação a todos os colaboradores e parceiros;
- Definir as medidas corretivas para as infrações contra esta Política;
- Indicar um Encarregado para atuar como canal de comunicação entre clientes, funcionários, prestadores de serviço, titulares de dados e a ANPD;
- Avaliar os incidentes de segurança e propor ações corretivas.

Colaboradores (funcionários CLTs, Estagiários, Prestadores de Serviço, Sócios) e Parceiros

- Conhecer e cumprir as normas estabelecidas nesta Política para a Segurança da Informação e os protocolos específicos de cada área para o tratamento de informações;
- Proteger informações contra acessos, divulgação, alteração e destruição não autorizados pela empresa;
- Cumprir as leis e normas que regem a propriedade intelectual;
- Não compartilhar informações da empresa ou de seus clientes com qualquer pessoa não autorizada;
- Não discutir assuntos confidenciais do trabalho em lugares públicos;
- Não emitir comentários ou opiniões relacionados a assuntos confidenciais de trabalho em redes sociais ou blogs;
- Informar qualquer violação desta Política ao Comitê de Segurança da Informação.

Colaboradores da Área de Tecnologia da Informação

- Configurar todos os equipamentos e sistemas com todos os controles necessários para que os requisitos de segurança estabelecidos por esta Política sejam cumpridos;
- Garantir que a identificação de qualquer pessoa no ambiente tecnológico seja única, pessoal e intransferível para que a responsabilidade de suas ações possa ser atribuída;
- Gerar logs e trilhas de auditorias para que falhas ou tentativas de fraudes possam ser identificadas;
- Segregar ao máximo as permissões de acesso das funções administrativas e operacionais, para restringir ao mínimo a possibilidade de pessoas eliminarem rastros de suas próprias ações;
- Planejar e fornecer recursos para armazenamento, processamento e acesso necessários que garantam a segurança estabelecida por esta Política;

- Estabelecer regras para a instalação de software e uso de hardware não homologado pela empresa e realizar auditorias periódicas para garantir o cumprimento destas regras;
- Restringir canais pelos quais circulam informações de terceiros, notadamente clientes e prestadores de serviços, e evitar a utilização de grupos de e-mails ou disparos internos em massa de informações e dados de terceiros;
- Garantir o bloqueio completo de acesso de usuários desligados ou sujeitos a medidas restritivas, quando solicitado formalmente.

Violação da Política de Segurança da Informação

Qualquer violação deve ser informada ao Comitê de Segurança da MAPS, que deverá investigar e determinar as medidas necessárias, visando correção da falha, alteração de processos, adaptação da Política e/ou imposição de ações corretivas aos envolvidos.

A violação das diretrizes estabelecidas nesta Política pode expor os envolvidos a advertências, rescisão do contrato e às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir. São exemplos de violações sujeitas a sanções: uso ilegal de software, tentativa de acesso a dados ou sistemas sem autorização, divulgação de informações de clientes ou da empresa, introdução de vírus no ambiente tecnológico da empresa.

POSSÍVEIS INCIDENTES DE SEGURANÇA

Toda violação a esta Política deve ser informada ao Comitê de Segurança da MAPS, mas nem toda violação implica um incidente de segurança.

No caso de uma possível violação dos requisitos de segurança de dados ("incidente de proteção de dados"), a MAPS tem obrigações de investigação,

informação e mitigação de danos. Um incidente de proteção de dados é uma violação de dados pessoais se houver uma violação de segurança que leve à destruição ilegal, alteração, divulgação não autorizada ou uso de dados pessoais. Quando a violação de dados pessoais puder implicar um risco para os direitos e liberdades dos Titulares, o Comitê de Segurança da MAPS deve geralmente ser informado da violação em até 72 horas após a sua detecção inicial. Se a violação de dados pessoais puder resultar em alto risco para os direitos e liberdades dos Titulares, eles e/ou o cliente controlador dos dados, devem ser notificados no menor prazo possível.

Incidentes de Segurança em aplicação, softwares ou ambientes da MAPS devem ser investigados independentemente de qualquer culpa da MAPS e mesmo que decorrente de mau uso por clientes e/ou terceiros. Um relatório simplificado deve ser produzido contendo descrição, causa e possíveis efeitos. A equipe responsável deve registrar documentalmente diagnósticos necessários e horas dispendidas na solução do Incidente.

Avaliação de Impacto na Proteção de Dados

A MAPS deve, ao introduzir novos processos, ou no caso de uma mudança significativa ao processamento existente, avaliar se esse processamento representa alto risco para a privacidade dos titulares de dados. A natureza, escopo, contexto e finalidade do processamento de dados devem ser levados em consideração. Como parte da análise de risco, o departamento responsável realiza uma avaliação do impacto do processamento planejado sobre a proteção de dados pessoais (avaliação de impacto na proteção de dados). Avaliação de atendimento a clientes e a utilização de estrutura da

MAPS por esses clientes deve ser feita de forma constante, especialmente por colaboradores da área de Tecnologia da Informação.

A conformidade com esta política e as leis de proteção de dados aplicáveis será revisada regularmente pelo Comitê de Segurança e por meio de auditorias de proteção de dados e outras verificações. Clientes e terceiros que confiem dados à MAPS poderão solicitar – e executar auditorias de proteção de dados em processamento de dados internos, de acordo com disposições contratuais. O responsável por acompanhar a auditoria de terceiros deve zelar para que as informações auditadas sejam exclusivamente aquelas relacionadas ao escopo da auditoria, mantendo a segurança e confidencialidade de informações de outros clientes. Acordos de confidencialidade devem ser celebrados preferencialmente antes das auditorias externas, caso essa confidencialidade já não tenha sido indicada em contrato.

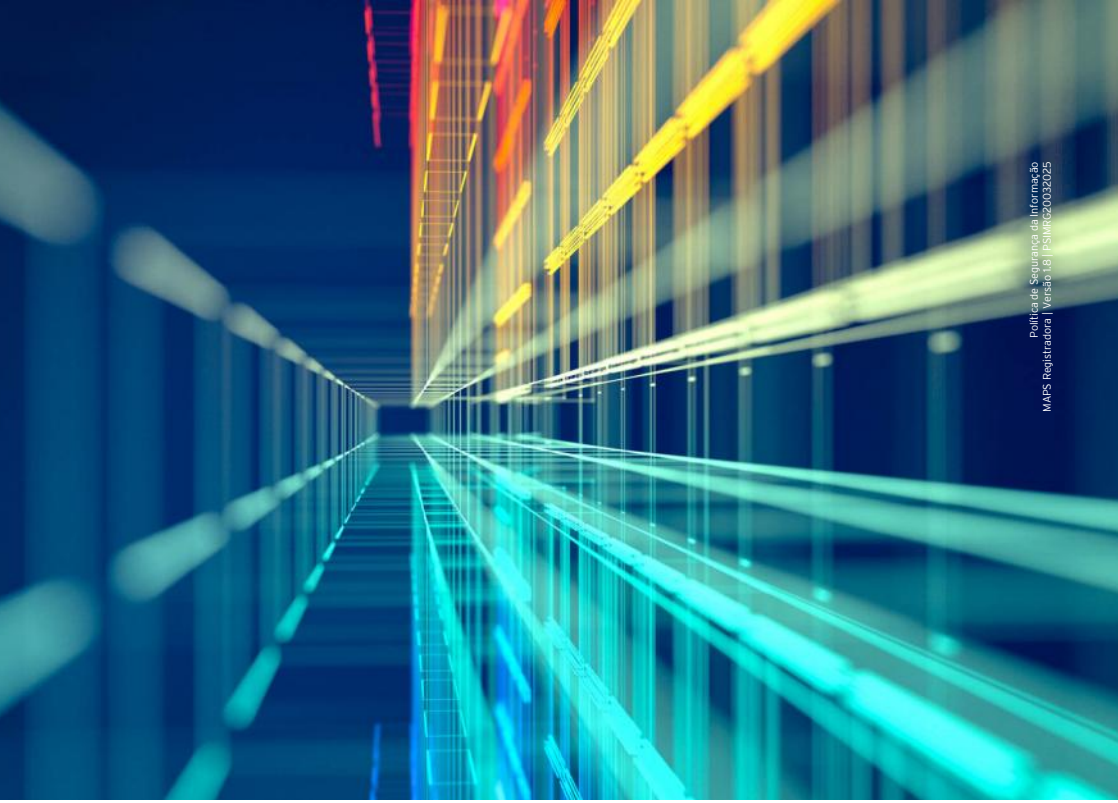
Processamento de Dados por Terceiros

A MAPS deve sempre identificar nas relações quem são os Titulares dos Dados, quem é o Controlador e quem é o Operador. A MAPS atuará como Operador de dados e informações de seus clientes apenas na medida das atividades que venha a prestar a esses clientes. A MAPS deve requerer – e auxiliar na medida do necessário – aos clientes que promovam o adequado tratamento de dados dos titulares de dados (os clientes dos clientes) nas plataformas, softwares e ambientes cedidos pela MAPS.

Esclarecimentos

O Comitê de Segurança da MAPS é a instância responsável por garantir que os requisitos legais e os contidos nesta Política sejam cumpridos. Dentro de sua área de responsabilidade, cada equipe terá um responsável por garantir que medidas organizacionais e técnicas estejam em vigor para que qualquer processamento de dados seja realizado de acordo com os requisitos de proteção de dados. A conformidade com esses requisitos é responsabilidade de todos.

Em caso de dúvida, contate o Comitê de Segurança no e-mail: **csi@maps.com.br**



maps registradora

Rua Afonso Celso, 552 / 6º andar
Vila Mariana / São Paulo / SP / 04119-002
+55 11 5085-7000
contato@mapsregistradora.com.br
www.mapsregistradora.com.br