SUMÁRIO

## 1. OBJETIVO

Formalizar os conceitos e as diretrizes da Segurança da Informação da **TERCILIO MARCHETTI IND E COM DE AUTOPEÇAS LTDA "MOLAS MARCHETTI"** que visam à proteção dos ativos de informação de modo garantir a confidencialidade, integridade e disponibilidade das informações, bem como a privacidade e proteção de dados pessoais[1].

## 2. ABRANGÊNCIA

Esta Política destina-se a todos os colaboradores, parceiros, fornecedores, prestadores de serviços das empresas do grupo **MOLAS MARCHETTI**:

- **MARCHETTI ATACADISTA DE AUTOPEÇAS LTDA;**

## 3. DIRETRIZES E PRINCÍPIOS

Todas as políticas de segurança da informação precisam estar disponíveis em local acessível aos colaboradores e devem ser protegidas contra alterações. As políticas de segurança da informação são revisadas anualmente ou conforme necessidade.

### 3.1. Diretrizes para a proteção de dados pessoais

Com esta política a **MOLAS MARCHETTI** visa estabelecer diretrizes de proteção de dados, com vistas a:

- Estar em conformidade com as leis e regulamentações aplicáveis de proteção de dados pessoais e seguir as melhores práticas;

[1] Dado pessoal: informação relacionada à pessoa natural identificada ou identificável.

- Proteger os direitos dos colaboradores, clientes, fornecedores e parceiros contra os riscos de violações[2] de dados pessoais;
- Ser transparente com relação aos procedimentos no tratamento[3] de dados pessoais;
- Promover a conscientização em toda a empresa em relação à proteção de dados pessoais e questões de privacidade.

## 3.2. Princípios da Segurança da Informação

O compromisso com o tratamento adequado das informações da **MOLAS MARCHETTI**, está fundamentado nos seguintes princípios:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

## 3.3. Ciclo de Vida da Informação

Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

- Tratamento: é a etapa onde a informação é coletada, criada ou manipulada a fim de atingir as finalidades definidas para o tratamento.
- Armazenamento: consiste na guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.
- Transferência: ocorre quando a informação é transferida para um Operador[4] ou compartilhada com outro Controlador[5], não importando o meio no qual ela está armazenada.

---

[2] Violação de dados pessoais: uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

[3] Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- Descarte: essa fase refere-se à eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

## 4. RESPONSABILIDADES

Para efeito desta política, estabelece e esclarece abaixo as responsabilidades:

### 4.1. Conselho

É de responsabilidade do Conselho:

- Definir o encarregado de proteção de dados, o DPO - Data Protection Officer;
- Estabelecer o mandato do DPO;
- Garantir que a organização atenda os requisitos desta política e a Lei Geral de Proteção de Dados.

### 4.2. Diretoria

É de responsabilidade da Diretoria:

- Definir e aprovar a estrutura de governança para os assuntos de privacidade e proteção de dados;
- Fazer o monitoramento permanente e efetivo da implementação das iniciativas de privacidade, incluindo os eventos relacionados a vazamento de dados pessoais;
- Garantir que no orçamento estejam previstos os recursos necessários para a implementação e gerenciamento das iniciativas de privacidade.

---

[4] Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

[5] Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais.

### 4.3. Encarregado[6] de Proteção de Dados

É de responsabilidade do Encarregado de Proteção de Dados (DPO - Data Protection Officer):

- Garantir a cultura de proteção de dados na empresa, a partir de treinamentos e programas de capacitação sobre a importância da Segurança da Informação e Proteção de Dados;
- Investigar riscos e incidentes[7] de segurança;
- Garantir a privacidade como um padrão, e a incorporação de medidas de segurança, participando e orientando os projetos que envolvam Tratamento de dados pessoais a fim de validar a aderência aos requisitos da legislação e da regulamentação aplicáveis;
- Promover a evolução do programa de proteção de dados, identificando riscos e oportunidades de melhoria;
- Comunicar imediatamente incidentes de proteção de dados que causem danos aos direitos dos titulares de dados, para a ANPD e para os titulares de dados atingidos;
- Preparar os relatórios de impacto à proteção de dados pessoais caso solicitado pela ANPD;
- Monitorar as solicitações dos Titulares de dados pessoais a fim de garantir que sejam respondidas dentro do prazo.

### 4.4. Área de Tecnologia da Informação

É de responsabilidade da área de Tecnologia da Informação:

- Implementar salvaguardas e mecanismos de controle para proteção dos recursos de sistema em toda a empresa, reforçando os sistemas críticos quanto à segurança da informação;
- Garantir a correta configuração dos sistemas para que somente usuários autorizados tenham acesso à informação;
- Adotar medidas proativas a fim de detectar riscos ou anormalidades no sistema.

### 4.5. Gerência, Coordenação e Líderes de Processo

É de responsabilidade da gerência, coordenação e líderes de processo:

[6] Encarregado = DPO (Data Protection Officer): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
[7] Incidente: um incidente, evento ou atividade real ou suspeita que comprometa a segurança dos sistemas de TI da Empresa ou de seus dados.

- Garantir que seus liderados cumpram as regras internas de privacidade e atuem de acordo com esta política;
- Realizar treinamentos, programas de conscientização e comunicação do tema de privacidade de dados pessoais;
- Revisar e manter atualizado o mapeamento de dados pessoais, junto com o Encarregado de Proteção de Dados (DPO);
- Monitorar o cumprimento das regras internas de privacidade.

### 4.6. Colaboradores

É de responsabilidade dos Colaboradores:

- Respeitar esta política, o código de conduta e seguir todas as orientações sobre a privacidade e proteção de dados;
- Utilizar os equipamentos de informática e comunicação, sistemas e informações para a realização das atividades profissionais com responsabilidade. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços;
- Relatar qualquer risco ou incidente de segurança da informação e proteção de dados aos responsáveis.

## 5. COMUNICAÇÃO DE INCIDENTES

De forma geral um incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita, que afete os princípios da segurança da informação: confidencialidade, integridade e disponibilidade dos dados. Alguns exemplos de incidente de segurança são:

- Perda ou roubo de dispositivos físicos, tais como notebooks ou dispositivos de armazenamento;
- Perda ou roubo de documentos que contenham dados pessoais;
- Acesso não autorizado a dados pessoais;
- Divulgação invertida de dados pessoais em virtude de “erro humano”;
- Divulgação inadvertida de dados pessoais em virtude de golpe, como resultado de procedimentos inadequados de verificação de identidade.

Sempre que houver um incidente de segurança é dever daquele que o percebeu comunicar o incidente para o DPO (Data Protection Officer), através do canal lgpd@molasmarchetti.com.br

## 6. CONFORMIDADE DE FORNECEDORES

As empresas prestadoras de serviços e fornecedores que manuseiem dados ou informações sensíveis, que sejam relevantes para a condução de suas atividades operacionais, devem estar adequadas à Lei Geral de Proteção de Dados e estas devem garantir, em contrato (ou aditivo), que:

- Os dados transferidos para a empresa serão utilizados somente para os fins definidos no contrato de prestação de serviço e que não são utilizados para outros fins;
- Os dados armazenados estão seguros e que são seguidas as melhores práticas de Segurança da Informação e Proteção de Dados;
- Em caso de vazamento de dados, como Controlador, será comunicado imediatamente para que possa tomar as devidas ações junto à ANPD.

## 7. DESCARTE DE DOCUMENTOS FÍSICOS

A proteção de dados pessoais extrapola os meios digitais devendo ser aplicada também sobre os dados em meios físicos, como cópias de contrato, formulários de clientes, dados de cartão de crédito, entre outros.

Assim, sempre que estes documentos tenham cumprido sua finalidade é necessário que sejam descartados de forma a garantir a proteção de dados. Abaixo as orientações de como se devem descartar alguns documentos:

- Cópias de Contratos – picotados através de uma fragmentadora de papel.
- [Outros documentos] – picotados através de uma fragmentadora de papel.

Em caso de dúvida procure o DPO (Data Protection Officer).

## 8. ATENDIMENTO AOS TITULARES

A Lei Geral de Proteção de Dados estipula alguns direitos aos titulares de dados que devem ser atendidos pelas empresas, são eles:

- Direito de conhecer o encarregado de dados - A LGPD determina que o encarregado deva ter sua identidade e seus dados para contato identificado publicamente;
- Direito à informação - O titular de dados pessoais tem direito a informações que dizem respeito à finalidade do tratamento, à sua forma de operação, aos agentes envolvidos e aos direitos que poderá exercer contra o controlador, as quais deverão ser apresentadas de forma clara, adequada e ostensiva;
- Direito a solicitações de providência - titular o direito de solicitar providências em relação aos seus dados mediante requisição, a qualquer momento e sem custos, tais como:
    - Confirmação da existência de tratamento;
    - Acesso aos dados pessoais objeto de tratamento;
    - Correção de dados incompletos, inexatos ou desatualizados;
    - Entre outros.

A **divulgação dos dados do Encarregado de Dados,** bem como **todas as informações sobre os tratamentos de dados realizados e como o titular pode solicitar providências**, deve ser solicitado/requerido **unicamente** através do e-mail: lgpd@molasmarchetti.com.br. Desta forma, teremos o registro de todas as movimentações inerente à LGPD.

## 9. GESTÃO DE RISCOS

Risco é a combinação da probabilidade de determinado evento ocorrer e o seu impacto no ativo e na operação da empresa, onde:

- Ativo é qualquer coisa que tenha valor para a organização (pessoas, equipamentos, sistemas, etc.);
- Evento é quando uma ameaça explora uma ou mais vulnerabilidades associadas a um ativo;
- Probabilidade consiste na medição de o quão provável é a ocorrência de um evento;
- Impacto traz a dimensão das consequências decorrentes do evento para o negócio caso determinada ameaça venha a explorar uma vulnerabilidade.

A avaliação de riscos é realizada sobre a lista de ativos, onde são identificados os possíveis eventos de proteção de dados e segurança da informação, que são avaliados quanto à probabilidade e impacto conforme as definições abaixo:

| PROBABILIDADE | | CRITÉRIOS |
|---|---|---|
| BAIXO | 1 | Pouco provável que aconteça. Pode ser que aconteça esporadicamente. |

| | | |
|---|---|---|
| MÉDIO | 2 | Pode ser que aconteça uma vez durante o ano. |
| ALTO | 3 | Pode acontecer com certa frequência. |

| IMPACTO | | CRITÉRIOS |
|---|---|---|
| BAIXO | 1 | Acontecimentos que não produzam desconforto aos titulares de dados. Sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. |
| MÉDIO | 2 | Acontecimentos que produzam desconforto aos titulares. Sem prejuízos financeiros e sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. |
| ALTO | 3 | Acontecimentos que produzam restrição às liberdades civis e aos direitos fundamentais dos titulares. |

Essas definições resultam na matriz de risco, que é uma tabela de duas dimensões: probabilidade e impacto, por meio da qual é possível calcular e visualizar a classificação do risco e, com isso, identificar quais são os riscos que devem receber mais atenção.

| MATRIZ DE RISCO | IMPACTO | | |
|---|---|---|---|
| PROBABILIDADE | BAIXO | MÉDIO | ALTO |
| BAIXO | 1 | 2 | 3 |
| MÉDIO | 2 | 4 | 6 |
| ALTO | 3 | 6 | 9 |

A partir da classificação dos riscos conforme a matriz de risco é identificado, quais riscos são mais críticos e determinada a estratégia de tratamento que podem ser:

- Diminuir o risco: esta opção inclui a implementação de salvaguardas (controles) – por exemplo: implantar sistemas de firewall, antivírus etc.
- Evitar o risco: parar de realizar certas tarefas ou processos se eles incorrerem em riscos que são muito grandes para mitigar com quaisquer outras opções – por exemplo: proibir a entrada de smartphones na área de desenvolvimento e pesquisa e a proibição de confecção de vídeos internos da área produtiva. Compartilhar o risco: significa você transferir o risco para outra parte – por exemplo: mudar seu servidor local para um data center, assim são diminuídos os riscos físicos

a que ele está exposto. Esta opção, por si só, pode não ser suficiente, então a melhor estratégia é usá-la em conjunto com uma das opções anteriores.

- Aceitar o risco: neste caso, a sua organização aceita o risco sem fazer nada a respeito. Esta opção deveria ser usada apenas se os custos de mitigação forem maiores do que o dano que um incidente poderia causar.

Após concluídas as ações de tratamento de riscos, é feita uma nova avaliação dos riscos para calcular o risco residual.

A avaliação de riscos é revisada anualmente ou na aquisição de um novo ativo.

## 10. PLANO DE RESPOSTA AS INCIDENTES GRAVES

O objetivo deste plano é reagir de forma rápida e assertiva a incidente de segurança que violam os direitos dos titulares de dados de modo a limitar seus danos, reduzir o tempo de recuperação, evitar ou diminuir possíveis custos e aumentar a transparência e confiança dos titulares quanto ao tratamento dos seus dados pessoais. Observando as seguintes fases:

### 10.1. Constituição do Comitê de Crise

Sempre que identificado um incidente de segurança, constitui-se o comitê de crise formado pelos integrantes: da Diretoria, responsável pelo setor de TI, o Encarregado de Dados e o responsável pelas ações de Marketing e comunicação corporativa. Este comitê terá a duração necessária para superar a crise e será liderado pela Presidência da empresa.

O trabalho do Comitê deve prever as seguintes atividades que podem ser adaptadas conforme o caso.

- Definir o problema para ter clareza sobre o que exatamente está acontecendo. Qual é o grupo de titulares foi afetado, a extensão do problema e quais os tipos de dados foram afetados;
- Levantar informações relevantes para identificar os fatos, descartar boatos, conversar com quem for diretamente responsável pelo problema e entender o que realmente aconteceu a fim de definir o que poderá ser feito;
- Centralizar a comunicação para que todas as comunicações acerca do incidente partam deste comitê. Tal medida se faz indispensável para minimizar informações desencontradas;

- Comunicar o mais breve possível e com frequência, o público interno e externo com informações relevantes, a fim de demonstrar transparência nas ações e mantê-los seguros de que o problema está sendo tratado com todo o cuidado e responsabilidade;
- Definir as estratégias de mídia mais adequadas para que a comunicação chegue aos titulares atingidos pelo incidente.

### 10.2. Ação imediata para interromper ou minimizar o incidente

O primeiro passo para a interrupção do incidente é avaliar se existem planos de contingência formalizados para tomar as ações já previstas para o tipo de incidente.

Caso o incidente não esteja previsto neste documento, é necessário avaliar com rapidez as possíveis ações para interrompê-lo, sempre levando em consideração o menor impacto nos direitos dos titulares.

### 10.3. Investigar o incidente

A liderança sobre o processo de investigação do incidente é do Encarregado de Dados, que deverá buscar o apoio de todas as áreas da empresa para esclarecer o ocorrido.

A área de TI deve auxiliar no rastreamento e investigação das questões de segurança assim como para analisar os sistemas comprometidos para levantar a extensão dos danos.

### 10.4. Restaurar os recursos afetados

Novamente o primeiro ponto de consulta para as ações a serem tomadas deve ser o Plano de Contingências, se houver.

Caso o incidente não tenha sido previsto em nenhum destes dois documentos, devem-se levantar as possíveis ações e levar para a decisão do comitê de crise.

### 10.5. Comunicar o incidente

Imagem, reputação e credibilidade são ativos muito importantes para qualquer negócio. Assim, determinar as estratégias de mídia e comunicação é atribuição do Comitê de Crise, que será responsável por elaborar as mensagens chaves, as quais devem incluir informações sobre o que aconteceu, o que a organização está fazendo a respeito e como está cooperando com as autoridades relevantes.

## 10.6. Comunicar titulares

Primeira comunicação: num primeiro momento, é possível, que não se tenham todas as informações sobre o incidente, porém, para uma maior transparência na relação com os titulares de dados deve-se fazer uma comunicação informando que se está ciente do problema e que está tomando todas as providências para resolver a questão.

Por exemplo:

“Apesar de todas as ações de Segurança da Informação e Proteção de Dados que promovemos, fomos vítimas de um incidente de vazamento de dados”. Ainda não temos informações suficientes para determinar a extensão do problema, porém já tomamos as seguintes ações a fim de contê-lo:

[citar as ações]

Pautamos nossa atuamos na Ética e Transparência, por isso nosso objetivo é deixar tudo esclarecido o mais breve possível. “Outras comunicações serão enviadas com o desenrolar dos fatos.”

Outras comunicações: Todas as outras comunicações com os titulares de dados deverão ser definidas pelo Comitê de Crise, levando-se em conta todo o cenário do incidente.

## 10.7. Comunicar a Agência Nacional de Proteção de Dados

A LGPD define que a comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I. A descrição da natureza dos dados pessoais afetados;
II. As informações sobre os titulares envolvidos;

III. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV. Os riscos relacionados ao incidente;
V. Os motivos da demora, no caso de a comunicação não ter sido imediata;
VI. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I. Ampla divulgação do fato em meios de comunicação;
II. Medidas para reverter ou mitigar os efeitos do incidente.

## 11. DEFINIÇÃO DO ENCARREGADO DE DADOS (DPO)

A Lei Geral de Proteção de Dados determina que o encarregado deverá ter sua identidade e seus dados para contato identificados publicamente. O DPO (Data Protection Officer) será nomeado (a) através de ata do Conselho de Administração, com período de mandato estabelecido, e independentemente do (a) selecionado (a), os temas relacionados à LGPD e esta política, deverão ser tratados através do e-mail: lgpd@molasmarchetti.com.br de forma a evidenciar e registrar todas as ocorrências.

## 12. DOCUMENTOS RELACIONADOS OU COMPLEMENTARES

Fazem parte desta política:

- a Política de Privacidade e Proteção de Dados Pessoais

- a Política de Privacidade de Navegação no Site

Obs.: Nas políticas acima referenciadas, será alterado somente o nome da empresa do grupo.

Estas políticas estão segregadas por empresa do grupo **MOLAS MARCHETTI** em seus websites:

www.molasmarchetti.com.br

## 13. REVISÕES

***** FIM *****