Política de Segurança da Informação, Cibernética e LGPD da Trivèlla M3 Investimentos S.A.

Versão – outubro de 2021.

Av. Cândido de Abreu, 470
Sala 2210, Neo Business
Curitiba - PR, Brasil
80530-000

+55 41 3121 0800
contato@tm3.capital
www.tm3.capital

1. Introdução

A Política de Segurança da Informação, Cibernética e LGPD da Trivèlla M3 Investimentos S.A., denominada neste documento "TM3 Capital" trata a informação como um ativo que possui grande valor para a TM3 Capital, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. Todo e qualquer usuário de recursos computadorizados tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos da TM3 Capital.

2. Objetivos

A Política de Segurança da Informação, Cibernética e LGPD da TM3 Capital, têm como objetivo estabelecer os fundamentos e diretrizes, a serem obrigatoriamente observados pela TM3 Capital e todos os seus colaboradores, no qual que assegurem a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e audibilidade da informação necessária para a realização do negócio da TM3 Capital, observando a natureza das operações, a complexidade dos produtos, dos serviços, das atividades e processos, bem como o porte, modelo de negócio e a sensibilidade dos dados e das informações sob responsabilidade da TM3 Capital.

3. Abrangência

A Política de Segurança da Informação, Cibernética e LGPD da TM3 Capital deve estar disposta de maneira que seu conteúdo possa ser consultado a qualquer momento e aplica-se a todos os funcionários e prestadores de serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da TM3 Capital, ou o acesso a informações pertencentes à TM3 Capital.

4. Vigência, Aprovação e Revisão

A presente Política entra em vigor na data de sua publicação e deverá ser revista e, se necessário, atualizada pelo Compliance no mínimo a cada 24 meses (vinte e quatro meses). Serão utilizadas como base para sua atualização as legislações, instruções normativas e regulamentações vigentes na data da sua revisão.

A aprovação desta Política, e posteriores atualizações, será a cargo da Diretoria Executiva da TM3 Capital. Também é de competência da Diretoria Executiva tomar as decisões administrativas referentes aos casos de descumprimento da Política.

5. Regulamentação Aplicável

- Resolução CVM nº 21/21;

- Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros;
- Guia Anbima de Cibersegurança;
- Lei nº 13.709/18 - Lei de Proteção de Dados Pessoais (LGPD) e alterações dadas pela Lei nº 13.853/19.

6. Ativos de Informação

A TM3 Capital considera como ativos de informação todas as informações, disponíveis em qualquer meio, utilizadas ou manipuladas nas operações da empresa, bem como todos os sistemas, equipamentos e instalações onde estas informações são manuseadas ou armazenadas.

As informações podem ser apresentadas nas mais distintas formas escritas, faladas, transmitidas, digitadas, armazenadas ou processadas em qualquer equipamento, papel, telefone, programa de computador, base de dados ou outro meio existente.

Seja qual for o estado ou o meio pelo qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com as normas definidas neste documento.

Para que não haja dúvidas, a TM3 Capital define como ativos de informação os seguintes itens:

- As informações criadas, processadas, acessadas, manuseadas e/ou armazenadas em qualquer meio ou sistema de informação da TM3 Capital;
- Os computadores, equipamentos, softwares, banco de dados, redes de comunicações e serviços de tecnologia utilizados pela empresa em suas operações, ou qualquer outro recurso, informático ou não, que seja utilizado nas atividades da empresa onde haja manipulação ou armazenamento de informações;
- As instalações em que estão localizados os equipamentos, sistemas, documentos ou informações da TM3 Capital;
- Processos e controles internos que sejam parte da rotina das áreas de negócio da TM3 Capital; e
- Governança da Gestão de Risco quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Dessa forma, os princípios de segurança da informação, cujos objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Assim, a TM3 Capital preserva suas informações quanto a:

Confidencialidade: Garantir que as informações sejam acessadas apenas por pessoas autorizadas;

Integridade: Garantir que as informações, tanto em sistemas quanto em bancos de dados, estejam em um formato verdadeiro e correto para seus propósitos originais;

Disponibilidade: Garantir que as informações e os recursos estejam disponíveis para aqueles que precisam delas quando necessário;

Acesso Controlado: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. A ameaça à segurança acontece se há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

7. Classificação da Informação

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

a. Informação Pública

É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e pelo público em geral.

b. Informação Interna

É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

c. Informação Confidencial

É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada desta informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

d. Informação Restrita

É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou pela área a que pertence. A divulgação não autorizada desta informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo gerente/supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

Dados dos Funcionários

A TM3 Capital se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários que porventura sejam armazenados serão considerados dados confidenciais e não serão usados para fins diferentes daqueles para os quais foram coletados. Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso, a lista de endereços eletrônicos (e-mails) usados pelos funcionários.

Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da empresa, sem prévia e expressa autorização por parte da Diretoria. Mesmo que seja autorizado o armazenamento destes dados, a empresa não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos servidores da empresa, e jamais poderão fazer parte da rotina de backup da empresa. Ainda, os funcionários se comprometem a não realizar a instalação de softwares nos computadores da empresa sem que exista autorização prévia para tal.

Admissão e demissão de funcionários/temporários/estagiários

Os responsáveis por Recrutamento e Seleção de Pessoal da TM3 Capital deverão informar ao profissional designado do setor de Informática sobre toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da empresa. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de informática.

Cabe ao setor solicitante pela contratação realizar o preenchimento do *checklist* para autorização de acessos do profissional recrutado e posterior envio e comunicação ao profissional designado do setor de informática sobre as rotinas a que o novo contratado terá direito de acesso.

No caso de temporários e/ou estagiários, deverá também ser informado o tempo em que o mesmo prestará serviço para a TM3 Capital, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas à autorização de seu acesso ao sistema. No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação, Cibernética e LGPD da TM3 Capital. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

8. Gerenciamento da Segurança Cibernética

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o

compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger a rede, os computadores, os sistemas e os dados de ataques ou acessos não autorizados.

O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

Há diversas razões para que esses ataques ocorram e os principais motivos são:

I. obter recursos financeiros;

II. roubar e manipular informações;

III. obter informações privilegiadas;

IV. sabotagem à instituição;

V. disseminar falsas notícias; e

VI. disseminar o caos.

A segurança cibernética deve garantir:

I. a segurança dos sistemas e dos bancos de dados;

II. o gerenciamento das pessoas autorizadas;

III. a segurança dos sistemas e informações que estão na nuvem;

IV. a segurança para todos os dispositivos/equipamentos;

V. o planejamento da continuidade do negócio; e

VI. o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

São exemplos de consequências/danos que podem ser causados pela falha na segurança cibernética:

I. risco de imagem;

II. risco de continuidade do negócio; e

III. prejuízos financeiros.

No que se refere especificamente à segurança cibernética, a TM3 Capital identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

Malware: softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);

Engenharia social: métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

Invasões (advanced persistent threats): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base na informação acima, a TM3 Capital avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e restabelecimento da segurança devida.

9. Regras Gerais de Segurança e de Uso de Tecnologia

São regras gerais para uso de tecnologia na TM3 Capital:

- Quando o usuário se comunicar através de recursos de tecnologia da TM3 Capital a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da empresa;
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia da TM3 Capital devem ser legais, estar de acordo com o Código de Ética, e devem contribuir para as atividades profissionais do usuário;
- O uso dos recursos de tecnologia da TM3 Capital pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente;
- Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados;
- Os recursos de tecnologia da TM3 Capital, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização;
- Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de Riscos e Controles Internos;
- Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura da TM3 Capital;
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de infraestrutura da TM3 Capital;

- É desabilitado ao usuário implantar ou alterar componentes físicos no computador;
- É implantada a proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);
- É implantado o "log-off" automático por inatividade durante o período de 24 horas.

Programas Ilegais

A empresa respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de programas ilegais (sem licenciamento) na TM3 Capital.

Os usuários não podem, em hipótese alguma, instalar qualquer "software" (programa) nos equipamentos da empresa sem autorização prévia e expressa. Periodicamente, o setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados se responsabilizam perante a Companhia por quaisquer problemas ou prejuízos causados oriundos desta ação, estando sujeitos às sanções previstas neste documento.

Permissões e Senhas

Todo usuário, para acessar os dados da rede da TM3 Capital, deverá possuir um login e senha previamente cadastrados pelo pessoal de Informática. Quem deve fornecer os dados referentes aos direitos do usuário é o responsável direto pela sua chefia. Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da TM3 Capital, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual se recomenda ser alterada imediatamente após o primeiro login e, após isso, a cada 180 (cento e oitenta) dias. Por segurança, a área de Informática recomenda que as senhas tenham: letra, número e caracteres especiais, critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Compartilhamento de Dados

Não é permitido o compartilhamento de pastas nos computadores e desktops da empresa sem autorização prévia. Todos os dados deverão ser armazenados nos servidores da rede, e a

autorização para acessá-los deverá ser fornecida pelo setor de Informática. Os compartilhamentos de impressoras devem estar sujeitos às autorizações de acesso do setor de Informática. Não é permitido, na empresa, o compartilhamento de dispositivos móveis tais como pen-drives e outros.

Backup (Cópia de Segurança dos Dados)

Todos os dados da empresa deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do setor de Informática e deverão ser feitas diariamente em um disco a parte e semanalmente em um servidor externo. O backup externo não tem risco de vazamento porque é criptografado. Ao final de cada mês, também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do Sistema Integrado.

Cópias de Segurança de Arquivos em Desktops

Não é política da TM3 Capital o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede.

Nestes e em outros casos, o pessoal de Informática deverá alertar ao usuário que ele deve fazer backup dos dados de sua máquina periodicamente.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da TM3 Capital.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da TM3 Capital, o setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

Segurança e Integridade dos dados

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

Acesso à Internet

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na TM3 Capital. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pelo setor de Informática, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Direção da TM3 Capital, com base nas melhores práticas. Não é permitido instalar programas provenientes da Internet nos microcomputadores da TM3 Capital sem expressa anuência do profissional designado para o setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais e extensões necessárias para uso de certificado digital. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licenças de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- de conteúdo pornográfico ou relacionado a sexo;
- que defendam atividades ilegais;
- que menosprezem, depreciem ou incitem o preconceito a determinados grupos ;
- que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da TM3 Capital;
- que promovam discussão pública sobre os negócios da TM3 Capital, a menos que autorizado pela Diretoria;
- que possibilitem a distribuição de informações de nível “Interno” ou “Confidencial”;
- que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

Uso do Correio Eletrônico (e-mail)

O correio eletrônico fornecido pela TM3 Capital é um instrumento de comunicação interna e externa para a realização do negócio da TM3 Capital. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da TM3 Capital, não podem ser contrárias à legislação vigente e nem aos princípios éticos da TM3 Capital.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- contenham declarações difamatórias e linguagem ofensiva;
- possam trazer prejuízos a outras pessoas;
- sejam hostis e inúteis;
- sejam relativas a qualquer “corrente” de e-mail;
- possam prejudicar a imagem da organização;
- possam prejudicar a imagem de outras empresas ou de clientes;
- sejam incoerentes com as políticas da TM3 Capital.

Para incluir um novo usuário no correio eletrônico, a respectiva gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Uso do WhatsApp para Fins Profissionais

Todos os colaboradores que utilizarem a ferramenta de WhatsApp para fins profissionais, deverão respeitar as normas e procedimentos descrito nesta Política, bem como o Código de Ética e Conduta e a Política de Compliance da TM3 Capital.

É terminantemente proibido trafegar documentos oficiais, informações não autorizadas pelo Compliance e qualquer outro conteúdo que infrinja diretriz da TM3 Capita via WhatsApp.

Sistemas de Telecomunicações

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da TM3 Capital, assim como, o uso de eventuais ramais virtuais instalados nos computadores, são de responsabilidade do setor de Informática, de acordo com as definições da Diretoria da TM3 Capital.

Uso de Antivírus

Todo arquivo em mídia não proveniente da TM3 Capital deve ser verificado por programa antivírus. Todo arquivo recebido/obtido através do ambiente Internet deve ser verificado pelo setor de Informática e por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede. O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Política de Segurança *Cloud* ou de Segurança em Nuvem

O arquivamento de dados em nuvens se insere num modelo de gestão compartilhada de dados, no qual torna-se necessária a contratação de uma pessoa jurídica provedora de nuvem, corresponsável, portanto, pela segurança de TI da TM3 Capital. Para tanto, devem ser analisadas as políticas preconizadas pelos principais fornecedores de nuvens a fim de se determinar, desde já, quais são as principais responsabilidades que se encontram sob a alçada de cada um, seja este a contratante, como a TM3 Capital, ou a contratada, a provedora de *cloud*. A prioridade de escolha da TM3 Capital recairá sempre em provedores de nuvens certificados por organização externa competente.

Programa de Gerenciamento de Incidentes de Tecnologia da Informação (TI)

De acordo com as boas práticas em gerenciamento de serviços de TI, um incidente é a interrupção não planejada de um serviço de TI ou a redução da qualidade do serviço prestado.

O Programa de Gerenciamento de Incidentes da TM3 Capital tem o objetivo de retomar um serviço o mais breve possível, causando o mínimo de danos ao negócio, de forma a mantê-lo no nível correntemente praticado por suas áreas de frente. Referido programa será composto pelas seguintes etapas:

- **Identificação de Incidentes:** o reconhecimento de incidentes da TM3 Capital dar-se-á por meio de sistemas de monitoramento internos, e pelos próprios usuários e clientes, que se comunicarão com a Diretoria de Compliance, por telefone ou e-mail.

- **Registro de Incidentes:** A ferramenta de controle de incidentes adotada pela TM3 Capital será uma planilha para fins de registro dos mesmos e de suas respectivas soluções, de modo a estabelecer uma base de dados para correções e prevenções futuras.

- **Categorização de Incidentes:** a Diretoria de Compliance classificará o chamado recebido por (a) tipo: (1) trata-se de um incidente ou uma requisição; e (2) consiste em um chamado de hardware ou software? e (b) a qual serviço do catálogo o incidente estará relacionado?

- **Priorização de Incidentes:** Trata-se de definir se o incidente deverá ser atendido imediatamente ou se poderá esperar um pouco, utilizando-se critérios relacionados à urgência e ao impacto. Um incidente urgente é aquele que precisa ser atendido rapidamente, enquanto um incidente impactante é aquele que poderá gerar grandes riscos ao negócio da TM3 Capital. Os incidentes poderão, ainda, ser classificados de acordo com um dos seguintes níveis de priorização: “muito baixo”, “baixo”, “normal”, “alto” e “muito alto”.

- **Diagnóstico Inicial de Incidentes:** Busca-se aqui, de fato, entender o incidente que foi reportado, de forma a abarcar todo o processo de procura por uma solução que realmente resolva o chamado de incidente efetuado por usuário do armazenamento em nuvem da TM3 Capital. Realizar-se-á uma análise da base de dados de incidentes da TM3 Capital destinada a ser utilizada como fonte de conhecimento para solução dos mesmos.

- **Escalada de Incidentes:** Caso o encarregado de resolver o incidente não tenha êxito na consecução dessa tarefa, a mesma será atribuída a um segundo nível de suporte, nos termos dos manuais detidos pelo provedor do armazenamento em nuvem contratado pela TM3 Capital.

- **Resolução de Incidentes:** Ocorre quando os chamados são realmente solucionados, seja pelo primeiro ou segundo níveis de atendimento, quando devem ser registradas as informações relevantes sobre o incidente e sua respectiva resolução.

- **Fechamento de Incidentes:** Trata-se do encerramento do chamado de incidente, que deve ser registrado na base de dados para futuras consultas.

Identificação dos Riscos

A empresa prestadora de serviços de TI é a responsável pelo mapeamento dos riscos internos e externos, dos equipamentos e softwares utilizados pela TM3 Capital.

A Diretoria de Compliance da TM3 Capital é responsável pela análise dos riscos mapeados e pela implantação/investimento dos processos que precisam de proteção e monitoramento.

Ações de Prevenção e Proteção

Todo o procedimento operacional é monitorado por empresa prestadora de serviços de TI, especializada em TI.

Monitoramento e Testes

A empresa prestadora de serviços de TI é a responsável pelo monitoramento e emite relatórios mensais que medem a disponibilidade dos servidores e das estações de trabalho, contendo a relação das atualizações realizadas e possíveis pontos de vulnerabilidades, serviços do sistema operacional e atualizações dos antivírus.

Plano de Respostas

A capacidade e efetividade do plano de resposta é vital para proteger as informações e os recursos de informação da TM3 Capital, clientes e usuários.

Todo o procedimento operacional é monitorado. Os recursos de TI são monitorados por sistemas automatizados que fornecem informações atualizadas sobre a indisponibilidade dos serviços com registro de incidentes para providências e encaminhamento de soluções e está preparada para possibilitar um plano de resposta de forma ágil e consistente.

Caso a TM3 Capital sofra algum ataque cibernético que ocasione a perda de acesso aos sistemas, os responsáveis por cada área estão autorizados a acionar a equipe de *help desk* da empresa prestadora de serviços de TI e ativar os acessos aos sistemas de back-up em nuvem da TM3 Capital, de forma que todo o trabalho operacional possa ser mantido.

10. Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados (LGPD) estabelece regras sobre como os dados pessoais (de pessoa física) devem ser tratados nos meios físicos ou digitais.

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 é considerada como tratamento de dados pessoais.

A LGPD determina que qualquer atividade de tratamento de dados pessoais deve respeitar a privacidade do titular envolvido. Dessa forma, a atividade deve trazer informações claras, precisas e de fácil acesso sobre:

- Como os dados pessoais serão tratados;
- Para qual finalidade esses dados serão usados;
- Quais são as medidas aplicadas para a segurança dessas informações;
- Quais direitos o titular envolvido tem sobre os seus dados pessoais.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

- **Finalidade:** propósitos legítimos, específicos, explícitos e informados ao titular.
- **Adequação:** compatibilidade do tratamento com finalidades informadas ao titular.
- **Necessidade:** limitação ao mínimo necessário para realização de suas finalidades.
- **Livre Acesso:** garantia, aos titulares, de consulta facilitada e gratuita.
- **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados.
- **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis.
- **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger dados.
- **Prevenção:** adoção de medidas para prevenir ocorrência de danos face ao tratamento dos dados pessoais.
- **Não discriminação:** impossibilidade de realização do tratamento com fins discriminatórios.
- **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar observância e cumprimento das normas de proteção de dados pessoais e eficácia dessas medidas.

A LGPD garante de forma não absoluta, o direito ao acesso, exclusão, revogação, dentre outros. Assim, qualquer atividade de tratamento que envolva dados pessoais deverá observar as regras trazidas pela LGPD (apresentadas em forma de princípios) e estar apta a atender todos os direitos garantidos aos titulares envolvidos.

Em geral os dados poderão ser tratados quando:

- Mediante fornecimento de consentimento do titular;
- Para cumprimento de obrigação legal ou regulatório pelo controlador;

- Pela administração pública, para tratamento e uso compartilhado de dados necessários à execução de políticas públicas;
- Para estudos por órgão de pesquisa, garantida, sempre que possível, anonimização dos dados pessoais;
- Quando necessário, para execução de contrato ou procedimento preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Para exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Para proteção da vida ou da incolumidade física do titular ou terceiro;
- Para tutela da saúde, em procedimento realizado por profissionais da área de saúde ou entidades sanitárias;
- Quando necessário atender interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam proteção dos dados pessoais;
- Para proteção do crédito.

Esta lei também atua extraterritorialmente, quando:

- A coleta e/ou o tratamento dos dados ocorreu em território nacional;
- Os dados são tratados para ofertar ou fornecer bens/serviços;
- A TM3 Capital, prezando pela segurança de seus clientes, adotou procedimentos internos para atender a todas as exigências da LGPD.

A LGPD protege o tratamento de dados das Pessoas físicas ou jurídicas, de direito público ou privado, que tratem dados pessoais no Brasil ou que coletem dados no Brasil ou, ainda, quando o tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a titulares localizados no Brasil, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

Perfis e Nomenclaturas

Titular: Pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento.

Controlador: Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado: 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).

Finalidade do Tratamento de Dados

Dentre outros, o tratamento dos dados pessoais cadastrais objetiva:

- Possibilitar o contato para fins de relacionamento comercial;
- Identificar e prevenir eventuais ameaças de segurança;
- Avaliar estatísticas;
- Enviar informes e/ou divulgações sobre os fundos de investimento e serviços;
- Possibilitar a estruturação, teste, classificação de seu perfil de Investidor visando informar-lhes sobre fundos de investimentos adequados ou não ao seu perfil de Investidor;
- Aprimorar e/ou corrigir problemas sistêmicos;
- Permitir o atendimento aos Usuários para que todos, inclusive você, possam entrar em contato com a TM3 Capital sempre que possível, e o contrário também.

Objetivo da Lei Geral de Proteção de Dados

O objetivo da lei é proteger os direitos de liberdade e privacidade dos titulares de dados pessoais.

Aplicabilidade da LGPD

A LGPD aplica-se a operações de processamento de dados que ocorrem no território brasileiro, mas também a operações de processamento de dados ocorrendo fora do território quando:

- Dados pessoais são coletados no Brasil;
- Os dados estão relacionados a indivíduos localizados no território brasileiro;
- Os dados são utilizados com o objetivo de oferecer produtos e/ou serviços ao público brasileiro.

O que são considerados como Dados Pessoais

Dados pessoais são informações que permitem identificar o indivíduo de forma direta (RG, CPF, endereço residencial etc.) ou indireta (dados registrados durante seus acessos em aplicativos e sites). Esses dados podem ser de clientes, ex-clientes, funcionários, ex-funcionários ou terceiros.

Serão necessários, no mínimo, os dados abaixo para o tratamento supracitado, indispensáveis ao cumprimento de obrigação legal ou regulatória:

- Nome completo do cliente, dos pais e do cônjuge, caso nos seja informado;
- Data de nascimento;

- Número e cópia da Carteira de Identidade (RG), caso nos seja encaminhado;
- Número e cópia do Cadastro de Pessoas Físicas (CPF), caso nos seja encaminhado;
- Número e cópia da Carteira Nacional de Habilitação (CNH), caso nos seja encaminhado;
- Estado civil;
- Nível de instrução ou escolaridade;
- Endereços completos e cópia do comprovante, caso nos seja encaminhado;
- Números de telefones e endereços de e-mail;
- Banco, agência e número de contas bancárias;
- Nome de usuário e senha específicos, necessários ao uso dos serviços da TM3 Capital;
- Comunicação, verbal e/ou escrita, mantidas entre o cliente e a TM3 Capital.

Consentimento dos Dados

O consentimento de coleta de dados pessoais poderá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com a Lei.

A TM3 Capital irá referir-se a finalidades determinadas e serão nulas as autorizações genéricas para o tratamento de dados pessoais.

É considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Havendo mudanças da finalidade para o tratamento de dados pessoais não compatível com o consentimento original, o titular deverá ser informado sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações.

Quando o tratamento for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos.

O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação

É dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular.

Direitos dos Titulares dos Dados Pessoais

O titular tem direito ao acesso facilitado às informações sobre o tratamento dos dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou em desconformidade com o disposto na Lei nº 13.709/18;
- Portabilidade de dados pessoais a outro fornecedor de produto ou serviço;
- eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Art. 16 da Lei nº 13.709;
- informação das entidades com as quais a TM3 Capital compartilhou o uso dos dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento do dado para o tratamento de dados pessoais, nos termos do § 5º do Art. 8º da Lei nº 13.709/18.

Por meio de medidas técnicas de segurança da informação detalhadas em 03 (três) pilares:

- **Processos:** São procedimentos padronizados de atuação. Sua implantação facilita a fiscalização evitando falhas técnicas;
- **Tecnologias:** São hardwares e softwares que têm o objetivo de salvaguardar ativos em formato de informação. Investimentos em novas tecnologias, como também em profissionais que saibam utilizá-las;
- **Pessoas:** São todos os indivíduos que interferem no tratamento de dados. Investimentos em treinamentos técnicos, em formação ética, daqueles que operam o tratamento de dados.

Agentes de Tratamento

Os agentes de tratamento adotam medidas de segurança, técnicas administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Legítimo Interesse

O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- apoio e promoção de atividades do controlador; e
- proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Somente poderá ser fundamentado para finalidades legítimas, consideradas a partir de situações concretas, que incluem o apoio e a promoção de atividades do responsável e, em relação ao titular, a proteção do exercício regular de seus direitos ou a prestação de serviços que o beneficiem, respeitadas as legítimas expectativas.

Dados Sensíveis

São informações que abrem margem para discriminação do indivíduo e que, portanto, merecem maior nível de proteção e cuidado. São dados que revelam convicção religiosa, opinião política, filiação a sindicato, origem étnica ou racial, informações referentes à saúde, vida sexual, genética e biometria, quando vinculados a uma pessoa natural.

A TM3 Capital não solicita dados de cartão de crédito .

O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

- quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
- cumprimento de obrigação legal ou regulatória pelo controlador;
- tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

- realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiros;
- tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
- tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (Redação dada pela Lei nº 13.853, de 2019); ou
- garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

No entanto, se a TM3 Capital passar a coletar dados sensíveis de forma habitual, esta Política será adaptada para atender às regras específicas previstas na LGPD para o tratamento de dados desta natureza.

Dados Anonimizados

Dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Porém, somente serão considerados dados pessoais, para os fins da LGPD, quando o processo de anonimização for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Poderão ser igualmente considerados como dados pessoais, para os fins da Lei, aqueles utilizados para a formação do perfil comportamental de uma determinada pessoa natural, se identificada.

A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessário para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

A pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa em nenhuma hipótese poderá revelar dados pessoais.

Crianças e Adolescentes

O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal, mediante todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança ou adolescente, consideradas as tecnologias disponíveis.

Armazenamento de Dados Pessoais

Os dados pessoais das pessoas físicas ficarão armazenados na nuvem da TM3 Capital e alocados em diretórios específicos, de acordo com o responsável pelo tratamento, sendo seu acesso segregado por tipo de função e autenticado por senha criptografada.

Nesse sentido, para proteger os Dados pessoais, são adotados os mais altos padrões de segurança tecnológica e física, a fim de evitar a perda, uso inadequado, acesso não autorizado, alteração e destruição dos mesmos.

Os dados pessoais permanecerão armazenados pelo tempo que for necessário, de acordo com a finalidade para a qual foram coletados e consentidos, sendo designado o respectivo prazo de armazenamento para cada Dado coletado pela TM3 Capital.

Para obter esta informação sobre o seu Dado, basta solicitá-la através do encarregado de LGPD, conforme descrito nesta política.

Compartilhamento de Dados Pessoais

Preservando a privacidade, segurança e confidencialidade das informações, a TM3 Capital poderá compartilhar os dados cadastrais registrados:

- Com parceiros estratégicos, prestadores de serviços e/ou fornecedores contratados;
- Para fins da Política de Privacidade ou em outras situações em que seu consentimento seja solicitado;
- Para cumprimento e execução de obrigações legais, regulatórias;
- Para cumprimento de solicitações e decisões de autoridades judiciais, administrativas ou arbitrais;
- Para investigação de possíveis infrações e análise de PLDFT à luz das Leis de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo e Anticorrupção (9.613/98, 12.683/12, 12.846/13, 13.260/16), entre outras normas correlatas;
- Para situações em que o compartilhamento seja necessário para criação, funcionamento e melhoria dos sistemas, das atividades, dos serviços da TM3 Capital

junto aos parceiros estratégicos, bem como para atendimento das finalidades previstas na Política de Privacidade da TM3 Capital.

Como Consultar e Alterar Informações sobre dados Pessoais

A pessoa física poderá consultar as informações sobre seus dados pessoais pelos Canais de Atendimento disponibilizados pela TM3 Capital.

Solicitar o Cancelamento de Tratamento dos Dados

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

- verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- fim do período de tratamento;
- comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do Art. 8º da Lei, resguardado o interesse público; ou
- determinação da autoridade nacional, quando houver violação ao disposto na Lei.

Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

A TM3 Capital manterá e tratará os dados pessoais cadastrados durante todo o período em que os mesmos forem pertinentes ao cumprimento regulatório e ao alcance das finalidades listadas nesta política.

Os Dados pessoais anonimizados, sem possibilidade de associação ao indivíduo, poderão ser mantidos por período indefinido.

Tratamento de Dados Pessoais Pelo Poder Público

O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do Art. 1º da Lei nº 12.527/11 (Lei de Acesso à Informação), se aplicável, deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

- sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
- seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do Art. 39.

Os dados e o uso compartilhado de dados pessoais pelo Poder Público, deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

No entanto, se a TM3 Capital passar a coletar dados pessoais de Poder Público de forma habitual, esta Política será adaptada para atender às regras específicas previstas na LGPD para o tratamento de dados desta natureza.

Transferência Internacional dos Dados

A TM3 Capital trata somente informações pessoais em território nacional e em países que possuem legislações semelhantes e equivalentes. Além disso, mantém cláusulas específicas para assegurar o correto tratamento, alinhadas com as leis e regulamentações brasileiras.

Controlador e Operador

O controlador e o operador da TM3 Capital manterão o registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Encarregado Pelo Tratamento de Dados Pessoais (DPO)

O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

As atividades do encarregado consistem em:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da autoridade nacional e adotar providências;
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O Encarregado pelo Tratamento de Dados Pessoais (DPO) da TM3 Capital é a pessoa responsável por assegurar o cumprimento da Lei Geral de Proteção de Dados.

O Encarregado pelo Tratamento de Dados Pessoais é responsável por receber e endereçar reclamações e comunicações dos Titulares de Dados, receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD), orientar os funcionários sobre as práticas de proteção de Dados Pessoais, e executar as demais atribuições determinadas pela TM3 Capital, ou estabelecidas em normas complementares.

Comunicação em Caso de Incidentes

O Encarregado pelo Tratamento de Dados Pessoais (DPO) da TM3 Capital comunicará a ANPD - Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Os danos são eventos capazes de compromissar alguns atributos de informações:

- Confidencialidade;
- Posse ou Controle;
- Integridade;
- Autenticidade;
- Disponibilidade;
- Utilidade.

A comunicação para a ANPD será feita em prazo razoável, conforme definido pela ANPD e deverá mencionar, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;

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

O órgão competente verificará a gravidade do incidente e poderá, caso necessário, determinar ao responsável a adoção de providências, tais como:

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

No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Segurança dos Dados

A TM3 Capital se responsabiliza pela manutenção de medidas de segurança, técnicas e administrativas visando proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou por tratamento inadequado ou ilícito.

Em conformidade ao Art. 48 da Lei nº 13.709/18, a TM3 Capital comunicará ao cliente e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante à pessoa física.

Os sistemas utilizados para o tratamento de dados pessoais da TM3 Capital são estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na Lei e às demais normas regulamentares.

Boas Práticas e Governança

Os controladores e operadores, no âmbito de suas competências pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular.

Na aplicação dos princípios, a TM3 Capital observará a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados.

O programa de governança em privacidade da TM3 Capital conterá, no mínimo, requisitos que:

- demonstrem o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- sejam aplicáveis a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- sejam adaptados à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- estabeleçam políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- tenham o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- estejam integrados à sua estrutura geral de governança e estabeleçam e apliquem mecanismos de supervisão internos e externos;
- contem com planos de resposta a incidentes e remediação; e
- sejam atualizados constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Para a TM3 Capital demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento da Lei.

Autoridade Nacional de Proteção de Dados (ANPD)

A ANPD, pelo Conselho Nacional de Proteção de Dados, é o órgão competente, integrante da administração pública federal indireta, submetido a regime autárquico especial e vinculado ao Ministério da Justiça.

A ANPD é composta pelo Conselho Diretor, como órgão máximo, e pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além das unidades especializadas para a aplicação da LGPD.

É caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira. O regulamento e a estrutura organizacional são aprovados por decreto do Presidente da República.

O Conselho Diretor será composto por 3 (três) conselheiros e decidirá por maioria:

- Zelar pela proteção dos dados pessoais, nos termos da legislação;
- Zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações;
- Elaborar diretrizes para Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- Atender petições de titular contra responsável;
- Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- Promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
- Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;
- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
- Dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, observado o respeito aos segredos comercial e industrial;
- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento e de proteção de dados pessoais previstos nesta Lei;
- Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante, assim como prestar contas sobre suas atividades e planejamento.

Relatório de Impacto à Proteção de Dados Pessoais

O relatório de impacto à proteção de dados (RIPD) é um instrumento de responsabilidade do controlador, pelo qual, em qualquer operação que envolva o tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos fundamentais, será realizada a descrição dos processos para mitigação de riscos e, concomitantemente, de responsabilidades, bem como medidas e salvaguardas.

A partir dos dados coletados, a TM3 Capital confeccionará um relatório de impacto à proteção a dados pessoais, no qual deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O relatório de impacto à proteção de dados (RIPD) deve ser incorporado dentro dos procedimentos de governança em privacidade corporativa do controlador, servindo como base para o cumprimento de diversos princípios da LGPD, especialmente:

- na finalidade, mediante a avaliação dos propósitos legítimos do tratamento; adequação, mediante a avaliação da compatibilidade das finalidades pretendidas de acordo com o contexto do tratamento; necessidade, limitando o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos;

- segurança, com a avaliação das medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão e prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

São elementos mínimos obrigatórios:

- descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

- avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos; avaliação dos riscos para os direitos e liberdades dos titulares dos direitos;

- avaliação das medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o Regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

A responsabilidade da decisão de quais operações de tratamento de dados deverão ser precedidas do relatório de impacto à proteção de dados pessoais, mediante a avaliação se poderão gerar riscos às liberdades civis e aos direitos fundamentais, é do controlador da TM3 Capital.

Para realização ou adoção de novas tecnologias que possam ser suscetíveis de implicar elevado risco para os direitos e liberdades dos titulares, tendo em vista a sua natureza, âmbito, contexto e finalidades, a TM3 Capital notadamente observará:

- avaliação sistemática e extensiva de aspectos pessoais relacionados às pessoas naturais, baseada no tratamento automatizado, incluindo a definição de perfis, quando as decisões produzirem efeitos jurídicos ou afetarem significativamente o titular dos dados;

- operações de tratamento em grande escala de categorias especiais de dados (sensíveis) ou de dados pessoais relacionados a condenações penais; ou
- monitoramento sistemático de ambientes de acesso público em grande escala.

Sigilo das Informações

O sigilo sobre as informações internas da TM3 Capital está em consonância com as diretrizes estabelecidas na Lei nº 13.709/18 e suas alterações dadas pela Lei nº 13.853/19, sobre Lei Geral de Proteção de Dados Pessoais – LGPD, nas quais consideram que as organizações são responsáveis por manter a Segurança e Sigilo de Dados de seus clientes.

Penalidades

O não cumprimento destas Políticas de Segurança da Informação, Cibernética e LGPD, implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

Considerações Finais

Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com o Compliance da TM3 Capital.

Manutenção dos Arquivos

A TM3 Capital manterá armazenados eletronicamente todos os arquivos pertinentes ao processo de Compliance desta política, pelo prazo mínimo de cinco anos, conforme legislação vigente.

Termo de Ciência e Acordo para Integrantes da TM3 Capital

Declaro que recebi, li e entendi as Políticas de Segurança da Informação e Segurança Cibernética da Trivèlla M3 Investimentos S.A. e estou ciente das diretrizes estabelecidas e sua relevância para mim e para a empresa. Comprometo-me a cumpri-las integralmente, sob pena de sujeitar-me às medidas punitivas e rescisórias previstas em contrato de trabalho e legislação vigente.

Nome Completo:

Data:

Assinatura:

Este termo consta de duas vias, uma para o Integrante e outra para a sua pasta

Av. Cândido de Abreu, 470
Sala 2210, Neo Business
Curitiba - PR, Brasil
80530-000

+55 41 3121 0800
contato@tm3.capital
www.tm3.capital