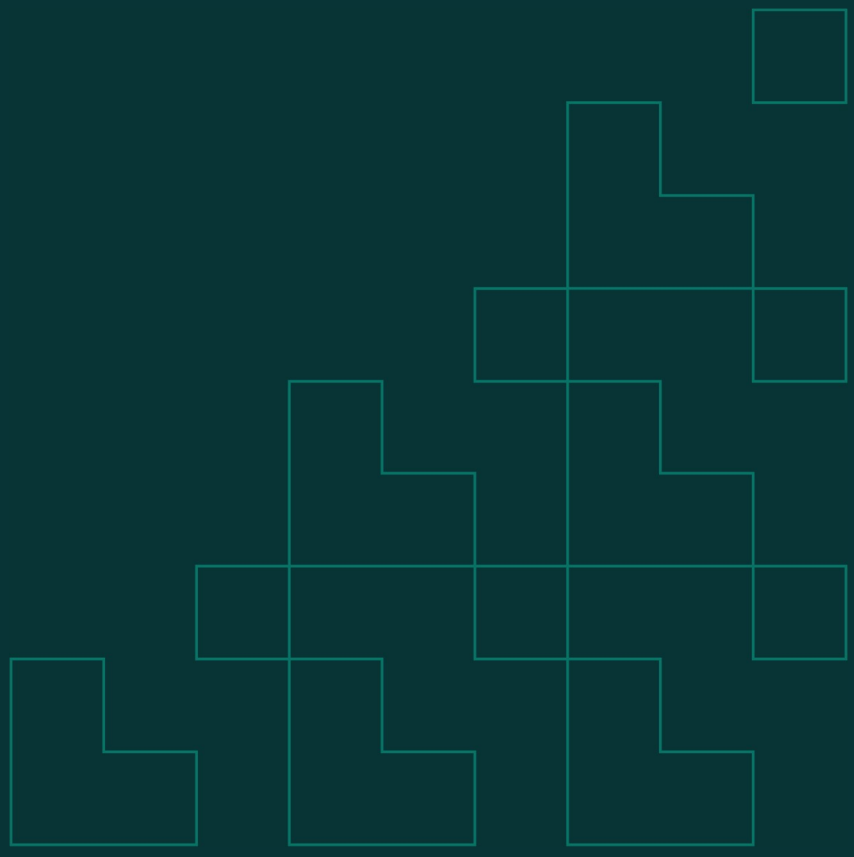
m square

Política de Privacidade e de Segurança Cibernética

(Parte Integrante do Manual de *Compliance*
da M Square Investimentos Ltda.).



M Square Investimentos Ltda.
Junho de 2022

m square

ANEXO X

POLÍTICA DE PRIVACIDADE E SEGURANÇA CIBERNÉTICA

A Política de Privacidade e Segurança Cibernética (“Política”) tem por objetivo estabeleceras regras, procedimentos e controles visando assegurar a segurança cibernética da M Square, bem como a confidencialidade, integridade, privacidade e disponibilidade dos dados e dos sistemas de informação utilizados pela Gestora. Esta Política de Privacidade e de Segurança da Informação ("Política") é uma declaração formal da empresa acerca de seu compromisso com a privacidade e a proteção das informações de sua propriedade e/ou sob sua guarda.

Deverá, assim, ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A Política está de acordo com as leis, regulamentação e autorregulação aplicáveis, incluindo a Lei nº 13.709/18 – Lei Geral de Proteção de Dados (“LGPD”), o Código ANBIMA de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros e o Guia de Cibersegurança de dez/2017, bem como as boas práticas de mercado.

1. Responsabilidade

1.1 Responsável pelo Programa de Governança em Privacidade e pela Segurança Cibernética

O(A) Diretor(a) de *Compliance* é responsável por esta Política, sendo o principal contato dentro da Gestora para tratar e responder questões de privacidade e segurança cibernética (“Responsável pela Segurança Cibernética e DPO”), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Os deveres e responsabilidades do(a) Diretor(a) de *Compliance*, na qualidade de Responsável pela Segurança Cibernética e DPO, incluem, dentre outros:

- Testar a eficácia dos controles (como por exemplo, backup e controle de infraestrutura) utilizados e informar ao Comitê de Privacidade e Segurança Cibernética os riscos residuais.
- Elaborar as políticas internas de segurança da informação e de proteção da privacidade e suas atualizações, garantindo mecanismos eficazes de monitoramento.
- Responder solicitações de Investidores, Colaboradores, terceiros e autoridades relacionadas à LGPD, podendo contar com o apoio de outros Colaboradores.
- Direcionar esforços e recursos propostos para a segurança da informação e a proteção da privacidade.

- Assegurar que seja realizada a configuração dos equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, bem como definir e assegurar a segregação das funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo, eliminando, ou ao menos reduzindo, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, mantendo evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Gestora.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Proteger continuamente todos os ativos de informação da Gestora contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Gestora.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Gestora, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Gestora.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Gestora operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Propor as metodologias e os processos específicos para a segurança da informação e para a proteção de Dados Pessoais sob responsabilidade da M Square, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Gestora.
- Garantir um backup em nuvem, devidamente criptografado com as rotinas de retenção (2 últimas semanas / cabeça de mês / cabeça de ano – por 5 anos).
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação e da proteção de Dados Pessoais para o negócio da Gestora, mediante campanhas, treinamentos e outros meios de endomarketing.

1.2 Comitê de Privacidade e Segurança Cibernética

O Comitê de Privacidade e Segurança Cibernética será composto pela equipe de *Compliance*, o qual poderá sempre que julgar necessário, convidar outros membros da área de TI para compor o respectivo comitê.

Ressaltamos que o Comitê de Privacidade e Segurança Cibernética ocorrerá dentro do Comitê de *Compliance* da M Square e se reunirá sempre que necessário para deliberar, além das matérias indicadas no Item 1.1 acima, sobre:

- Definição e revisão de quaisquer regras, normas e procedimentos internos adotados pela Gestora para o cumprimento das responsabilidades e obrigações listadas no item 2 desta Política, incluindo a constituição de manuais internos complementares desta Política.
- Avaliação dos riscos internos e externos, (*risk assessment*) identificados nos termos do item 4 desta Política.
- Estabelecer ações de prevenção, proteção e medidas internas em prevenção a ocorrência de ataque cibernético nos termos do item 5 desta política.
- Análise dos procedimentos de monitoramento e de testes periódicos nos termos do item 6 desta Política.
- Cumprimento Plano de Resposta a Incidentes quando o Responsável pela Segurança Cibernética e DPO tenha sido acionado devido a um potencial incidente envolvendo risco cibernético e/ou questões de privacidade, nos termos do item 6 desta Política.

1.3 Atribuições de Todos os Colaboradores

Caberá a todos os Colaboradores conhecer e adotar as definições desta Política, e seus deveres e responsabilidades na manutenção da segurança corporativa e da privacidade. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança cibernética ou a proteção de dados pessoais, o qual recorrerá a(o) Diretor(a) de *Compliance*, se for o caso.

Em caso de incidente que afete a privacidade e/ou a segurança cibernética da Gestora e/ou descumprimento desta Política, o Colaborador deverá comunicar imediatamente a(o) Diretor(a) de *Compliance*. Em caso de descumprimento, ainda que involuntário, o Colaborador responsável estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei, a exclusivo critério da Gestora.

2. Proteção da Privacidade e de Dados Pessoais

Este capítulo tem o objetivo de esclarecer as características, regras e finalidades do tratamento de dados pessoais realizados pela M Square para a prestação de seus serviços de gestão profissional de recursos de terceiros com foco em investimentos e produtos internacionais (“Serviços”).

Ao utilizar os Serviços da M Square, navegar e utilizar as funcionalidades de seu Website ou tornar-se um Colaborador, você, na qualidade de Investidor, parceiro, terceiro ou Colaborador, compreende e aceita guiar-se por esta Política. A M Square poderá alterar esta Política a qualquer tempo por meio de atualização publicada no Website, à qual você ficará vinculado.

2.1 O que são Dados Pessoais?

A lei define como "dado pessoal" qualquer informação relacionada a uma pessoa natural identificada ou identificável. Tal pessoa é o "titular" dos dados.

Alguns dados pessoais são considerados "sensíveis", recebendo maior proteção legal, dentre eles os de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural.

O tratamento de dados inclui toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2.2 De que forma a M Square coleta Dados Pessoais?

A M Square pode deter dados pessoais:

- de Investidores, de seus representantes e de potenciais clientes, fornecidos por escrito por meio de documentos de subscrição, questionários, documentos, ou, ainda, pessoalmente, por telefone ou via e-mail;
- Via recebimento e transferência de dados para parceiros, fornecedores e prestadores de serviços ("Parceiros");
- de potenciais candidatados fornecidos no processo de recrutamento; e/ou
- de Colaboradores fornecidos no processo de admissão.

2.3 Quais dados são tratados pela M Square e por quê?

A M Square realiza o tratamento dos dados pessoais, sobretudo, para a execução e melhoria dos Serviços, cumprimento de obrigações regulatórias e execução dos contratos de que é parte.

Como regra, a M Square não solicita dado pessoal sensível ou de indivíduos menores de 18 anos para a realização dos Serviços. É possível que alguns dados pessoais sensíveis sejam coletados em caso específicos, tal como de Colaboradores ou de seus dependentes para fins regulatórios. Desta forma,

nenhuma informação desta natureza deve ser fornecida à M Square a não ser que expressamente solicitada. Caso sejam fornecidos dados pessoais sensíveis por engano ou imprudência, será interpretado que o titular dos dados pessoais autorizou expressamente a M Square a eliminar ou anonimizar tais dados.

2.4 Como ocorre o compartilhamento de Dados Pessoais?

A M Square compartilha dados pessoais com Parceiros na estrita necessidade para execução dos Serviços, cumprimento de normas e funcionamento da Gestora.

Os serviços prestados pelos Parceiros são, primordialmente: (i) administração fiduciária de fundos de investimento; (ii) distribuição de cotas fundos de investimento; (iii) contabilidade e folha de pagamento de Colaboradores (iv) serviços de recrutamento e divulgação de vagas; e (v) serviços de tecnologia de informação.

Excepcionalmente, a M Square poderá compartilhar Dados Pessoais em outras hipóteses como: (i) venda, fusão ou aquisição de um negócio ou ativo; (ii) responder uma intimação ou ordem judicial, processo judicial ou autoridades regulatórias; (iii) suspeita de conduta potencialmente criminal ou fraudulenta; (iv) interesses legítimos da M Square, mediante prévia anonimização; e/ou (v) em outras situações excepcionais, mediante consentimento prévio do titular dos dados pessoais.

A M Square não compartilha dados pessoais para fins de marketing e não vende Dados Pessoais sob nenhuma hipótese.

2.5 Transferência internacional de Dados

A M Square realiza transferência internacional de dados pessoais com Parceiros localizados no exterior com o objetivo de viabilizar a prestação dos Serviços e cumprimento de obrigações regulatórias locais. Para isso, a M Square observa todos os requerimentos estabelecidos pela legislação aplicável e adota as melhores práticas de segurança e privacidade para garantir a integridade e confidencialidade de quaisquer dados pessoais de Investidores.

2.6 Eliminação e anonimização de Dados Pessoais?

A M Square mantém dados pessoais coletados após o término da prestação dos Serviços ou desligamento de Colaborador, conforme aplicável, pelo tempo exigido pela legislação aplicável ou para fins de cumprimento de seus deveres e direitos empresariais. Em alguns casos, os dados podem ser eliminados ou anonimizados antes do esperado, caso já não sejam mais necessários para finalidade para que foram coletados.

2.7 Direitos do Titular dos Dados Pessoais

Aqueles que fornecem seus Dados Pessoais à M Square, tem os seguintes direitos:

Direitos do Titular	
Acesso	Requerer cópia de ou confirmação de quais são os seus Dados Pessoais sob custódia da M Square.
Correção	Solicitar a correção de seus Dados Pessoais. Para efetivar a correção, a M Square checará a veracidade e titularidade dos dados fornecidos.
Anonimização, bloqueio ou eliminação	Requerer a suspensão temporária de qualquer operação de tratamento de seus Dados Pessoais e solicitar sua exclusão da base de dados da M Square quando entender que são desnecessários ou excessivos.
Portabilidade	Solicitar a transferência de seus Dados Pessoais a outro prestador de serviços, salvo Dados Pessoais já anonimizados ou eliminados pela M Square.
Exclusão	Requerer a exclusão de seus Dados Pessoais tratados com base no consentimento.
Compartilhamento	Ser informado acerca de todas as entidades com as quais seus Dados Pessoais são compartilhados. Para tanto, o titular poderá basear-se nesta Política.
Negativa ou Revogação do consentimento	Não consentir ou revogar seu consentimento acerca do tratamento de seus Dados Pessoais realizado pela M Square, ressalvado os casos em que não é necessário o consentimento para seu tratamento, sendo que o tratamento realizado previamente à solicitação continuará válido. Nesse caso, a M Square ficará impossibilitada de fornecer os serviços de comunicação e envio de formulários e newsletters do Website.

Os direitos acima podem ser exercidos mediante solicitação à M Square, a qualquer tempo e por qualquer razão pelo e-mail: Compliance@msquare.com.br.

A M Square alerta que a revogação dos consentimentos expressos nesta Política pode resultar na impossibilidade e inviabilização dos Serviços.

2.8 Cookies

Cookies são pequenos arquivos contendo informações enviados de um Website para o seu navegador, os quais são utilizados principalmente para identificar e armazenar informações.

A M Square utiliza Cookies para tarefas distintas, como oferecer uma navegação eficiente, recolher estatísticas, otimizar as funcionalidades e melhorar a experiência do usuário.

O período que o navegador armazena as informações provenientes dos Cookies, dependerá do tipo de Cookie, os quais geralmente possuem uma data de expiração.

Ao continuar navegando no Website, o usuário concorda com a nossa Política de Privacidade e de Segurança Cibernética.

2.9 Sites de terceiros

O Website poderá ter em seu conteúdo links de outros sites, o que não significa que esses sites sejam de propriedade ou operados pela M Square. Ao clicar nestes anúncios ou links e ser direcionado para o site destes anunciantes, deverão ser observadas as políticas e termos do site em questão.

2.10 Dúvidas ou solicitações

Dúvidas e solicitações acerca desta Política devem ser direcionadas a(o) Diretor(a) de *Compliance*, encarregado para os assuntos de LGDP, conforme abaixo:

Nome: Renata Silveira
Endereço: Av. Brig. Faria Lima, 3355, 10º andar
E-mail: Compliance@msquare.com.br.

3. Princípios da Segurança dos dados e dos sistemas de informação

O objetivo das regras sobre segurança cibernética da Gestora é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da Gestora devem assegurar:

- a 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);
- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e
- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da Gestora, observadas as regras de sigilo da

Política de Confidencialidade e Segurança da Informação constante no Manual de *Compliance* e o item sobre confidencialidade no Código de Ética da Gestora.

Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pela M Square pertence à Gestora. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da Gestora poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

A M Square exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4. Identificação/avaliação de riscos (*risk assessment*)

A M Square periodicamente, no mínimo uma vez ao ano, deverá identificar os riscos internos e externos, bem como os ativos de *hardware* e *software* e processos que precisam de proteção. Esse processo será conduzido pela Comitê de Privacidade e Segurança Cibernética, o qual deverá ser documentado pelo(a) Diretor(a) de *Compliance* com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Gestora e seus riscos de cibersegurança e de privacidade. A Gestora poderá contratar uma empresa terceirizada para tanto, caso a(o) Diretor(a) de *Compliance* julgue necessário e mediante aprovação do Comitê de Privacidade e de Segurança Cibernética.

Após a condução do referido processo, o Comitê de Privacidade e Segurança Cibernética deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Gestora, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade do evento acontecer.

Segue abaixo uma lista não exaustiva de riscos de segurança cibernética e de privacidade que podem ser identificados na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de *hackers*;
- Tratamento de dados em desconformidade com a LGPD;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em *link* malicioso (“*Phishing*”);

- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de *software* em contrariedade com as aprovações e condições estabelecidas nesta Política; ou
- Vazamento de informações e dados pessoais durante tráfego de dados não criptografados.

5. Ações de prevenção e proteção

A Gestora estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Todas as informações encontradas nos ambientes da M Square são tratadas como confidenciais e sigilosas, e as orientações de tratamento encontram-se na presente Política, no capítulo sobre a Política de Confidencialidade e Segurança da Informação e Comunicação com o Público no Manual de *Compliance*, e no capítulo sobre Código de Ética da Gestora, divulgados para todos os Colaboradores da Gestora, em especial os com acesso às informações e aos sistemas da Gestora, incluindo orientações que definem a maneira pela qual devem usar a tecnologia dentro da M Square.

5.1 Comunicações eletrônicas

Os Colaboradores devem observar que qualquer e-mail ou mensagem instantânea ("**MI**") que constitua um registro sobre qualquer atividade, transação ou negócio da Gestora é mantido pela M Square.

5.1.1 Mensagem Instantânea

A Gestora reconhece que, em determinados casos, a MI pode ser uma fonte valiosa de informação, bem como um método eficiente de comunicação. A Gestora, portanto, permite aos Colaboradores usar o recurso de MI para comunicações relacionadas a suas atividades enquanto as Mis são enviadas e recebidas usando a plataforma designada pela Gestora para tais comunicações (Microsoft Teams). Os Colaboradores são proibidos de usar uma plataforma não designada para enviar e receber MIs relacionadas às atividades de gestão.

5.1.2 Política de Retenção de Comunicações Eletrônicas

A Gestora implantou uma "**Política de Retenção de E-mail**" em que a Gestora tentará reter todos os e-mails e mensagens instantâneas. A Política de Retenção de E-mail da Gestora é composta por diversos fatores:

- O(A) Diretor(a) de *Compliance* é responsável pela supervisão da política;
- Os Colaboradores devem abster-se de conduzir suas atividades por meio de qualquer rede de comunicação não pré-aprovada pela Gestora (p.ex., e-mail externo, mensagem instantânea ou mensagem de texto não fornecido pela Gestora ao Colaborador ou que não possa ser capturado pelo sistema de retenção de e-mail);
- Todas as comunicações eletrônicas contempladas pelas exigências aplicáveis de manutenção de registro estão identificadas e preservadas da forma adequada;
- O descarte permanente de e-mails da rede da M Square deve ser conduzido de uma forma que proteja a confidencialidade, mediante prévia aprovação do(a) Diretor(a) de *Compliance*; e
- Todos os Colaboradores no momentos do início do vínculo com a Gestora, são informados sobre a Política de Retenção de Comunicações Eletrônicas.

5.1.3 Procedimentos Operacionais

O(A) Diretor de *Compliance* revisará a Política de Retenção de E-mail, quando necessário, para garantir que seus *backups* estejam funcionando e que a Gestora possa disponibilizar e-mails, caso solicitado por um regulador.

5.1.4 Uso de Ativos

A utilização dos ativos da M Square, incluindo computadores, telefones, Internet, programas de *mensagem* instantânea, e-mails e demais aparelhos se destina a fins profissionais, e deve ser feita com cuidado.

Infraestrutura

Todos os computadores da M Square são criptografados e gerenciados pelo MDM (*Mobile Device Management*) do *Office 365,* e o(a) detentor(a) dos acessos, poderá resetar o equipamento, com prévia autorização do(a) Diretor(a) de *Compliance*.

Os computadores da M Square são fornecidos para o exclusivo uso dos Colaboradores no desempenho de suas atividades profissionais, mediante assinatura de um Termo de Responsabilidade.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Documentos imprescindíveis para as atividades dos Colaboradores da Gestora deverão ser salvos no Sharepoint.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Os usuários não são administradores das máquinas, não tendo privilégios para acessar conteúdo no perfil de outro possível usuário logado.
- Os Colaboradores devem informar a(o) Diretor(a) de *Compliance*, por meio formal, qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da equipe de TI ou por terceiros devidamente contratados para o serviço.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização do(a) Diretor(a) de *Compliance*.
- Todas as contas deverão ter o *Two-factor authentication* - 2FA devidamente ativado.

5.1.5 Dispositivos Móveis

Considerando que deseja facilitar a mobilidade e o fluxo de informação entre seus Colaboradores, a M Square permite o uso de seus equipamentos portáteis. Por "dispositivo móvel", entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da Gestora, ou aprovado e permitido pelo(a) Diretor(a) de *Compliance*, como: *notebooks*, *smartphones* e *pen drives* (mediante prévia autorização/liberação).

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os Colaboradores que utilizem tais equipamentos.

Todo dispositivo móvel é gerenciado pelo MDM (*Mobile Device Management*) do *Office 365,* e, com isso, o(a) detentor(a) dos acessos poderá resetar o aparelho em padrão de fábrica, com prévia autorização do(a) Diretor(a) de *Compliance*.

O Colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na M Square, mesmo depois de terminado o vínculo contratual mantido com a Gestora.

Todo Colaborador deverá ter o *Two-factor authentication (2FA)* devidamente instalado na sua conta de e-mail e VPN.

É permitido o uso de rede banda larga de locais conhecidos pelo Colaborador como: sua casa, hotéis, fornecedores e clientes. O Colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará que assumiu todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à Gestora e/ou a terceiros.

5.1.6 Datacenter

O acesso de visitantes ou terceiros ao Datacenter somente poderá ser realizado com acompanhamento de um Colaborador autorizado. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer Colaborador responsável pela administração de liberação de acesso.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a autorização do(a) Diretor(a) de *Compliance*.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero ou inflamável.

No caso de desligamento de Colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de Colaboradores autorizados.

5.1.7 *Uso de e-mail*

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da M Square, inclusive que contenha fins políticos locais ou do país (propaganda política). O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente. Em nenhuma hipótese um Colaborador pode emitir uma opinião por e-mail em nome da M Square, salvo se expressamente autorizado para tanto pelo(a) Diretor(a) de *Compliance*.

Acrescentamos que é proibido aos Colaboradores o uso de e-mail da M Square para as seguintes atividades:

- Enviar mensagens (i) não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Gestora; (ii) pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar; (iii) que torne seu remetente e/ou a Gestora vulnerável a ações civis ou criminais; (iv) com informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação; (v) que inclua material protegido por direitos autorais sem a permissão do detentor dos direitos; (vi) que contenha Dados Pessoais de Investidores e Colaboradores, exceto quando autorizado por esta Política ou pelo(a) Diretor(a) de *Compliance*, nos termos desta Política;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a Gestora estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que (i) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Gestora; (ii) contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; (iii) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança, bem como que vise:
- obter acesso não autorizado a outro computador, servidor ou rede;
- interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- burlar qualquer sistema de segurança;
- vigiar secretamente ou assediar outro usuário;
- acessar informações confidenciais sem explícita autorização do proprietário;
- acessar indevidamente informações que possam causar prejuízos a qualquer pessoa.

As mensagens de e-mail deverão incluir assinatura com o seguinte formato: (i) nome do Colaborador, Nome da empresa, *Disclaimer*, Telefone(s) e Correio eletrônico, conforme especificado pela equipe de TI da Gestora.

5.1.8 *Uso da Internet*

Todas as regras atuais da M Square visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da Internet. Embora a conexão direta e permanente da rede corporativa com a Internet ofereça um grande potencial de benefícios, também propicia riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na Internet está sujeita a divulgação e auditoria. Portanto, a Gestora reserva-se o direito de monitorar e registrar todos os

acessos a ela, nos termos da legislação aplicável. Como mencionado, os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade da Gestora, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/Internet, estejam em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

A visualização de conteúdos que contenham dado discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física) obsceno, pornográfico ou ofensivo é terminantemente proibida.

Programas licenciados e instalados nos computadores, principalmente via Internet ("downloads"), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do(a) Diretor(a) de *Compliance*.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado poderá excluído pela equipe de TI. Os Colaboradores não poderão em hipótese alguma utilizar os recursos da Gestora para fazer o *download* ou distribuição de *software* ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. O *download* e a utilização de programas de jogos são proibidos.

Colaboradores com acesso à internet não poderão efetuar *upload* (subida) de qualquer *software* licenciado à M Square ou de dados de sua propriedade a Terceiros (conforme definido nesta Política) e clientes, sem expressa autorização do responsável pelo *software* ou pelos dados. Os Colaboradores não poderão utilizar os recursos da Gestora para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, *spam*, assédio, perturbação ou programas de controle de outros computadores.

O acesso a *softwares peer-to-peer* (Kazà, BitTorrent e afins) não serão permitidos. Já os serviços de *streaming* (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos, conforme definido pelo(a) Diretor(a) de *Compliance*. Não é permitido acesso a sites de proxy.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo superior. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Gestora cooperará ativamente com as autoridades competentes.

5.1.9 Identificação e uso de senhas

Observado o disposto na Política de Confidencialidade e Segurança da Informação, a senha e *login* para acesso aos dados contidos em todos os computadores corporativos, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

Todos os dispositivos de identificação utilizados na M Square, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a Gestora e a legislação (cível e criminal).

É também proibido o compartilhamento de login para funções de administração de sistemas. A Área Administrativa da M Square é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos Colaboradores.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários não possuem perfil de administrador. E as senhas deverão ter pelo menos 8 caracteres, sendo um deles, especial.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 5 (cinco) tentativas de acesso, a conta do usuário será bloqueada pelos próximos 30 minutos (caso não seja desbloqueada manualmente pelo administrador). Para o desbloqueio é necessário que o usuário entre em contato com a equipe de TI. Caso o Colaborador esqueça sua senha, ele deverá requisitar formalmente a troca, para que a equipe de TI realize o cadastro de uma nova senha. Deverá ser estabelecido um processo para a renovação de senha. Os usuários podem alterar a própria

senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Assim que algum usuário for demitido ou solicitar demissão, a Área Administrativa deverá imediatamente comunicar tal fato à equipe de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

5.1.10 Reprodução e *Descarte*

É terminantemente proibido aos Colaboradores fazer cópias ou imprimir arquivos usados, gerados ou disponíveis na rede da M Square e circular em ambientes externos a M Square com esses arquivos, uma vez que tais arquivos contêm informações consideradas confidenciais, conforme descrito no "Instrumento de Política Comercial" e "Compromisso de Responsabilidade e Confidencialidade" presentes no Anexo VIII e Anexo IX do Código de Ética, respectivamente.

A proibição acima não se aplica quando as cópias ou impressão de arquivos forem usadas para executar ou desenvolver negócios e interesses da M Square. Nestes casos, os Colaboradores em posse e guarda da cópia ou do arquivo impresso contendo as informações confidenciais serão diretamente responsáveis por sua boa conservação, integridade e manutenção de sua confidencialidade.

O descarte de informações confidenciais em meio digital ou físico deve ser feito de forma a impossibilitar sua recuperação.

Em consonância com as normas acima, os Colaboradores devem abster-se de utilizar *pen drives* ou qualquer website de compartilhamento de informações (e.g. Dropbox, Google Drive, etc.) discos ou quaisquer outras mídias que não exclusivamente para o desempenho de sua atividade na M Square.

Todas as informações que possibilitem a identificação de um Investidor da M Square devem permanecer em arquivos de acesso restrito, e somente poderão ser copiadas ou impressas para o atendimento dos interesses da M Square ou do próprio Investidor. Tal restrição não se aplica na eventualidade de cumprimento de ordem de autoridade judicial ou extrajudicial determinando a disponibilização de informações sobre eventual Investidor da M Square, cujo atendimento deverá ser previamente comunicado a(o) Diretor(a) de *Compliance*.

5.1.11 Conexão na Rede da M Square

É proibida a conexão de qualquer equipamento na rede da M Square sem a prévia autorização pelas áreas de informática e *Compliance*.

5.1.12 *Controles e Registros de Atividades*

A Gestora implementou controles robustos de acesso utilizando duplo fator de autenticação em seu sistema de e-mail, VPNs e nos sistemas críticos da M Square (Controle de acesso lógico adequado aos ativos da organização).

5.2 Procedimentos de Proteção de Dados e de Segurança Cibernética de Terceiros Contratados

Os fornecedores, prestadores de serviços e parceiros da M Square ("Terceiros") também podem representar uma fonte significativa de riscos de proteção de privacidade de dados e de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço e, assim como as demais contratações de Terceiros, envolve determinados riscos que devem ser levados em conta pela Gestora, demandando certos cuidados proporcionais a esta identificação de ameaças.

5.2.1 Avaliação dos Terceiros contratados

Nesse sentido, a área de *Compliance* da Gestora deverá verificar o conteúdo mínimo de *Compliance* em segurança cibernética de Terceiros que (i) gerem acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de computação em nuvem, (iii) tenham conexões lógicas (*links*) com a Gestora, (iv) tratam dados pessoais relacionados às atividades da M Square ou (iv) qualquer outros que a área de *Compliance* julgue que por qualquer motivo possa gerar risco de privacidade e de cibersegurança à Gestora, previamente à sua contratação, na forma do Anexo A desta Política.

Com base em tal verificação, o(a) Diretor(a) de *Compliance* avaliará a capacidade deles de evitar ataques cibernéticos e da potencial contratação, devendo a decisão sobre a contratação ficar formalizada, sendo periodicamente reavaliada.

5.2.2 Requisitos de segurança da informação nos contratos com Terceiros

A Gestora deverá incluir em contratos com Terceiros cláusulas de proteção de dados pessoais, requisitos de segurança da informação, bem como assegurar que os Terceiros contratados tenham políticas próprias de proteção de dados e de segurança cibernética e verificar a efetividade dos controles implementados pela empresa contratada para atender aos requisitos durante a vigência do contrato, na forma menciona acima.

6. Monitoramento e Testes Periódicos

Os mecanismos de supervisão para cada risco identificado no item 3 acima se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no

ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de históricos: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à Internet e aos sistemas críticos da Gestora; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Gestora; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

A M Square investe em ferramentas robustas para monitoramento do ambiente, como também, em equipe especializada através da implementação do Network Operation Center ("NOC") e periodicamente realiza a atualização de seus ativos, a qual é registrada em um sistema pertinente, com a geração de relatórios mensais. O NOC monitora todos os *backups*, os quais são testados através de visualização dos dados salvaguardados.

Para garantir as regras mencionadas nesta Política, a Gestora deverá:

- Implantar sistemas de monitoramento nos dispositivos corporativos, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Para os riscos associados a *Phishing*, conduzir treinamentos e campanhas periódicas, bem como testes de *Phishing*, ao menos anualmente;
- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e
- Testar a vulnerabilidade e penetração do Website da Gestora, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela M Square, ao menos anualmente.

Periodicamente, a Gestora revisa o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança de privacidade e cibersegurança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Gestora poderão ser acessados, caso o Comitê de Risco e *Compliance* julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

7. Plano de Resposta a Incidentes

A Gestora deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Contingência e Recuperação de Desastre, anexo ao Manual de *Compliance* da Gestora ("Plano"), considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave) e os descritos abaixo para os demais casos.

Os Colaboradores poderão reportar incidentes diretamente a(o) Diretor(a) de *Compliance* ou por meio do canal de reporte de incidentes: E-mail: *Compliance*@msquare.com.br.

7.1 Procedimento em caso de incidente

Uma vez que o(a) Diretor(a) de *Compliance* tenha sido acionado devido a um potencial incidente, este deverá convocar o Comitê de Privacidade e Segurança Cibernética.

Avaliação Inicial

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Comitê e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

Incidente Caracterizado

Se for caracterizado um incidente, devem os membros do Comitê tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, informar à CVM, ANBIMA, Agência Nacional de Proteção de Dados ("ANPD") ou outra autoridade competente, (ii) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa, em especial a Investidor ou Colaborador que tenha sido afetado; e (iv) houve prejuízo para a Gestora, algum Veículo de Investimento ou Investidor específico. Além disso, o Comitê, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

Recuperação

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um acompanhamento, conforme o caso, em

periodicidade a ser definida, com um sumário elaborado pelo(a) Diretor(a) de *Compliance* contendo as medidas a serem tomadas, responsabilidades e prazos.

Também deverá se avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações, tais como manifestação pública na mídia, com eventual contração de PR, enquanto que o Comitê de Investimentos verificará se todas as informações necessárias ao portfólio estão seguras e a área de gestão definirá se decisões de investimento são requeridas. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados ao Comitê. Terceiros relevantes deverão ser mantidos atualizados.

Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar ao *full Compliance*, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A Área de *Compliance* deverá registrar o histórico em local adequado, como o sistema de gerenciamento, Compli.ly.

8. Reciclagem e revisão

A Gestora deverá manter o programa de proteção de dados e de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização em privacidade e cibersegurança, com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger dados pessoais e outras informações como parte de suas responsabilidades por meio do Programa de Treinamento da Gestora.

O(A) Diretor(a) de *Compliance* realizará a revisão e atualização desta Política periodicamente, sempre que algum fato relevante ou evento motive sua revisão, conforme análise e decisão do(a) Diretor(a) de Compliance.

9. Termos e Definições

- Website – https://www.msquare.com/ e demais páginas deste domínio.

ANEXO A

MODELO DE DILIGÊNCIA COM TERCEIROS DO GRUPO TÉCNICO DE CIBERSEGURANÇA DA ANBIMA

CONTEÚDO MÍNIMO DE *COMPLIANCE* EM PRIVACIDADE E SEGURANÇA CIBERNÉTICA A SER VERIFICADO

Compliance	Respostas
1. A empresa tem políticas, programa e procedimentos formais relativos à proteção de Dados Pessoais, segurança da informação e cibersegurança? a. Se sim, é objeto de teste ou auditoria periódica? b. Se não, está em fase de elaboração? Qual é o prazo de finalização dele para devido envio à instituição contratante?	
2. A empresa apresenta plano de resposta a incidentes de cibersegurança?	
3. A empresa apresenta ações de conscientização, educação e formação de proteção de Dados Pessoais e de segurança da informação junto a seus funcionários?	
4. Quais são as ferramentas e os mecanismos utilizados para proteção de dados (incluindo Dados Pessoais) transacionados com a empresa contratante?	
5. Quais são as práticas aplicadas para detectar atividade não autorizadas nos sistemas utilizados? Solicitar também designação de responsável por detectar tais atividades e a quem se reporta.	
6. Na eventualidade de detecção de incidente de cibersegurança, o relato é feito por meio de canais de gestão apropriadas o mais rápido possível? Há comunicação a clientes e/ou reguladores (quando aplicável)?	
7. Se a empresa faz tratamento de Dados Pessoais: • A empresa possui um Data Protection Officer (DPO)?	

• A empresa possui conhecimento de como os Dados Pessoais tratados por ela são armazenados, processados e utilizados? • A empresa possui documentada a base legal que justifica o tratamento dos Dados Pessoais no âmbito de suas atividades? • Os empregados recebem treinamento sobre as disposições da LGPD? • Foi realizada na empresa auditoria ou avaliação de risco sob a perspectiva da LGPD recentemente? Se sim, quais foram as recomendações feitas e o que foi implementado até o momento?	
Favor disponibilizar os seguintes documentos: • Programa de segurança cibernética: se a organização segue políticas, programa e procedimentos formais relativos à segurança da informação e cibersegurança, recomenda-se solicitar envio da documentação à empresa contratante para avaliação e arquivamento. Solicitar também o último relatório de teste/auditoria periódica. • Se a empresa faz tratamento de Dados Pessoais: Política de Privacidade e/ou Proteção de Dados Pessoais: solicitar também declaração de que a empresa está em conformidade com a LGPD, inventário e fluxograma de Dados Pessoais e o último relatório de avaliação de risco realizado. • Certificações: solicitar envio de certificações que possam comprovar a devida capacidade técnica do prestador de serviço.	