POLÍTICA DE SEGURANÇA CIBERNÉTICA E CONFIDENCIALIDADE

São Paulo, 05 de março de 2026

SUMÁRIO

1. Objetivo

Esta Política tem por objetivo o adequado gerenciamento das informações de posse temporária ou de propriedade da DOMO.

2. Conceito de Informação Confidencial

Por Informação Confidencial entende-se toda e qualquer informação resguardada contra a revelação pública não autorizada, ou seja, informação eletrônica, escrita ou falada da qual o Colaborador tiver acesso dentro da Gestora, incluindo: dados da DOMO, das investidas dos Fundos geridos pela DOMO, seus sócios, diretores, Investidores e Colaboradores, bem como de relatórios de órgãos reguladores, autorreguladores e do poder público, dados de inspeções e fiscalizações, materiais de *marketing* e demais informações de propriedade da Gestora.

O dever de confidencialidade dos Colaboradores, com relação às informações que tiverem acesso dentro da Gestora, ou atreladas aos seus Investidores, subsiste nos casos de desligamento dos mesmos.

3. Controles de acesso a Informações Confidenciais

Todo acesso a diretórios e sistemas de informações da DOMO deve ser controlado pela área de Compliance. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pelo Diretor de Compliance.

O controle do acesso a sistemas de informações da DOMO levará em conta as seguintes premissas:

3.1. Utilização de identificador do Colaborador (ID do Colaborador);

3.2. Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil;

3.3. Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora;

3.4. Registro de log de acesso para inclusão, alteração e exclusão de toda e qualquer informação do ambiente tecnológico da Gestora; e

3.5. Permitir trilhas de auditoria.

4. Barreiras de controle de informações

Os Colaboradores detentores de Informações Confidenciais ou Privilegiadas, em função de seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações para os demais Colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas:

4.1. Os Colaboradores devem evitar circular em ambientes externos à DOMO com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, salvo se necessárias ao desenvolvimento do projeto e no interesse do Investidor, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso;

4.2. O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;

4.3. As informações que possibilitem a identificação de um Investidor da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da DOMO ou do próprio Investidor;

4.4. Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes, etc;

4.5. Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos;

4.6. A senha de acesso do Colaborador ao sistema da DOMO é pessoal e intransferível; e

4.7. O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora, e poderá ser monitorado pela área de Compliance sempre que necessário. O uso do e-mail corporativo para fins pessoais por parte dos Colaboradores será admitido desde que não haja impacto no desempenho de suas funções na Gestora.

5. Segregação das Atividades

Caso a DOMO venha desenvolver outra atividade no mercado de capitais, além da gestão de recursos de terceiros, essa nova atividade deverá ser totalmente segregada das atividades atualmente realizadas, salvo no que for expressamente permitido pela legislação em vigor.

No que tange à segregação das atividades do Diretor de Gestão, é importante ressaltar que sua independência é requisito essencial regulamentar e está intrinsecamente ligada à cultura da Gestora. Nesse sentido, tal Diretor não pode ser responsável por nenhuma outra atividade no mercado de capitais, na instituição ou fora dela.

6. Segurança Cibernética

Este tópico tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da DOMO, com o objetivo de garantir o adequado gerenciamento das

Informações Confidenciais, conforme estipulado pelo Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como seguindo as recomendações e diretrizes do Guia de Cibersegurança da ANBIMA, datado de junho de 2021.

A DOMO, com o propósito de manter a confidencialidade das informações, bem como garantir a integridade e disponibilidade destas, leva em consideração três aspectos básicos, quais sejam:

- Confidencialidade: somente pessoas devidamente autorizadas pela Gestora deverão ter acesso às informações;
- Integridade: somente alterações, supressões e adições autorizadas pela Gestora devem ser realizadas nas informações; e
- Disponibilidade: as informações devem estar disponíveis para as pessoas autorizadas, sempre que necessário.

6.1. Responsável por Questões de Cibersegurança

O Diretor de Compliance, assessorado pelo Sr William Silva, advisor da DOMO em assuntos de tecnologia, é o responsável imediato da DOMO para tratar de questões relacionadas a cibersegurança na Gestora.

6.2. Procedimetos de Segurança Cibernética

Cabe a DOMO atuar contra ameaças cibernéticas por meio das seguintes funções, no mínimo: ***(i)*** identificar/avaliar os riscos (*risk assessment*); ***(ii)*** atuar na prevenção e proteção; ***(iii)*** monitorar; ***(iv)*** elaborar plano de resposta a eventuais incidentes; e ***(v)*** governança.

(I) Identificação e Avaliação de Riscos (*Risk Assessment*):

Os principais riscos cibernéticos aos quais a Gestora está exposta, mas não se limitando, são:

- *Malware* (vírus, cavalo de troia, *spyware* e *ransomware*);
- Acesso indevido aos dados dos investidores;
- Acesso indevido aos dados das investidas;
- Cópias indevidas de documentos e/ou de informações confidenciais
- Acesso pessoal;
- Ataques de DDoS e botnets; e
- Invasões (*advanced persistent threats*).

A DOMO deve, ainda, continuamente identificar todos os ativos relevantes da Gestora (sejam eles equipamentos, sistemas, processos ou dados) usados para o correto funcionamento das atividades. As vulnerabilidades dos ativos identificados devem ser avaliadas, identificando-se as possíveis ameaças e o grau de exposição dos ativos a elas, bem como diferentes cenários devem ser considerados nessa avaliação.

Serão considerados também os possíveis impactos financeiros, operacionais e reputacionais, em caso de evento de segurança, assim como a expectativa de tal evento ocorrer. O processo de avaliação de riscos, assim, contemplará as atividades desenvolvidas por prestadores de serviços terceirizados, incluindo, mas não se limitando, aos serviços de nuvem.

A partir da identificação das vulnerabilidades, as informações confidenciais devem ser classificadas, permitindo com isso a implementação de processos para o devido manuseio, armazenamento, transporte e descarte dessas informações.

Nesse contexto, são ativos relevantes para a DOMO, mas sem se limitar:

- Equipamentos: computadores, pen drives e HDs;
- Sistemas: sistemas proprietários, site, sistemas contábeis, email e Google Workspace;
- Processos: pesquisa e avaliação de potenciais investidas.
- Dados: Informações Confidenciais.

(II) Prevenção e Proteção:

A DOMO possui regras para controlar o acesso aos equipamentos, sistemas, processos e dados da Gestora, bem como regras para concessão de senhas de acesso aos diferentes dispositivos, sistemas e rede.

Nesse contexto, os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto aos arquivos e sistemas internos são inventariados, todo o processo ocorre dentro do Google Workspace. Todo acesso a diretórios e sistemas de informações da DOMO deve ser controlado, mediante login e senha. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores que precisarem destas informações para realizar suas atividades, observada a devida segregação de funções, e após prévia autorização do Diretor de Compliance.

A senha que foi fornecida para acesso à rede de dados institucionais não deverá, em nenhuma hipótese, ser revelada a outra pessoa, podendo o Colaborador ser responsabilizado caso disponibilize a terceiros tais senhas para quaisquer fins.

Os Colaboradores da DOMO efetuam a troca de suas senhas periodicamente, de acordo com a política de senhas do Google Workspace.

As regras sobre senhas poderão ser modificadas a qualquer momento, em decorrência de avanços tecnológicos ou decisão interna da área de Compliance da DOMO, visando sempre o aprimoramento dos procedimentos, sistemas e da segurança das informações.

Todo conteúdo que está na rede pode ser acessado pela área de Compliance, caso haja necessidade, além disso, eventuais arquivos pessoais que vierem a ser salvos nos computadores oficiais da DOMO, poderão ser acessados caso o Diretor de Compliance identifique como necessário, sejam em processos de validações aleatórias, específicas e/ou em

caso de auditorias ou demandas regulatórias. Os demais Colaboradores têm acessos previamente definidos.

A DOMO realiza *backup* de todos os seus arquivos e sistemas em servidores de nuvem, os quais cumprem com as recomendações normativas de segurança da cibernética, inclusive para os casos de serviços em nuvem. A adequação de questões jurídicas também será avaliada, incluindo, mas não se limitando às cláusulas de confidencialidade e exigência de controles de segurança na própria estrutura dos terceiros.

(III) Monitoramentos

O monitoramento automático é realizado pelos sistemas do Google Workspace.

Existe também, on-line, monitoramento de eventuais tentativas de invasão ao sistema de arquivos da DOMO e, ainda, são realizados testes por meio de sistemas do Google Workspace. . O monitoramento dos controles de segurança adotará a abordagem baseada em risco, intensificado, assim, conforme o nível de risco se eleve.

Os relatórios gerados no mencionado monitoramento são utilizados como base para atualização das nossas prevenções e plano de resposta.

(IV) Plano de Resposta

Os Colaboradores deverão comunicar à área de Compliance quaisquer casos de violações às normas de segurança cibernética que tenham conhecimento. Toda violação ou desvio deve ser investigado para a determinação das medidas necessárias a serem adotadas, visando a correção da falha ou reestruturação de processos.

Nos casos em que houver violação desta Política ou das normas de Segurança da Informação por parte de Colaboradores, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar no desligamento e eventuais processos nas áreas criminal, cível e administrativa, caso aplicável.

A DOMO, em um evento envolvendo segurança cibernética, deverá iniciar o plano de resposta, conforme descrito abaixo:

(V) Avaliação e Medidas

Uma vez identificado um evento envolvendo a segurança cibernética, o Diretor de Compliance convocará para reunião o Comitê Executivo da DOMO e o representante de TI. O objetivo da reunião será a realização de uma análise dos fatos, seus motivos e consequências imediatas, baseadas na avaliação dos riscos anteriormente realizada, identificando desse modo a gravidade da situação, medidas necessárias a serem adotadas e áreas da DOMO a serem acionadas.

O Diretor de Compliance será responsável por coordenar a aplicação das medidas decididas em conjunto com o Comitê Executivo e com o representante de TI. Dentre as medidas imediatas, a depender do incidente ocorrido, deverá ainda ser dada publicidade do

fato aos órgãos competentes como CVM, ANBIMA, COAF, ANPD, etc e, sendo aplicável, informar a polícia via boletim de ocorrência ou queixa crime do fato.

Ademais, cada área da DOMO deve adotar as seguintes providências quando forem acionadas pelo Diretor de Compliance:

Área de TI ou Empresa de TI terceirizada sob Supervisão da área de Compliance:

- Verificação e Auditoria dos Logs;
- Criação de laudo pericial contendo as informações que foram potencialmente vazadas;
- Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
- Desinstalação de software;
- Execução de varreduras offline para descobrir quaisquer ameaças adicionais;
- Formatação e reconstrução do sistema operacional;
- Substituição física de dispositivos de armazenamento;
- Reconstrução de sistemas e redes;
- Restauração de dados provenientes do backup realizado diariamente;
- Avaliação da necessidade ou não de continuação das operações da DOMO de forma remota, considerando o nível de comprometimento das instalações/sistemas do escritório;
- Entre outros.

Área de Compliance

- Criação de relatório baseado no laudo pericial elaborado pela área de TI, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;
- Em caso de confirmação do incidente de segurança e eventual vazamento de Informações Confidenciais, elaborar notificação aos clientes afetados e autoridades competentes informando o ocorrido.

BackOffice

- Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da DOMO;
- Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo incidente ocorrido deverá ser devidamente classificado por nível de severidade (em baixo, médio ou alto), considerando o grau de comprometimento provocado nas atividades da Gestora, bem como será arquivado e documentado pela área de Compliance, sendo ainda formalizado no Relatório de Controles Internos da DOMO.

Além disso, a DOMO deverá definir os passos a serem tomados junto à área de TI a fim de evitar que o incidente ocorra novamente.

Day After

Após identificado o problema e realizadas as atitudes necessárias, serão definidas novas medidas a serem tomadas, incluindo, mas não se limitando, ***(i)*** o retorno ao uso dos equipamentos e rede atacados, quando for o caso; e ***(ii)*** implementação de contingências, físicas ou em nuvem, quando aplicável.

Todo histórico relacionado ao incidente deverá ser arquivado como evidência para eventuais esclarecimentos futuros.

Governança

A DOMO realizará testes periódicos de segurança para os sistemas de informações (sem se limitar a estes, mas em especial para os meios eletrônicos), no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

O treinamento sobre segurança de informação fará parte do treinamento inicial e periódico da DOMO, conforme programa de treinamento anual, o qual deverá, dentre outros, assegurar que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações aqui previstos, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e má interpretação das normas e procedimentos.

O Diretor de Compliance, responsável pela segurança cibernética, realizará revisão desta Política anualmente ou sempre que este julgar necessário.

Eventuais comunicações e questionamentos devem ser enviados para a área de Compliance por meio do e-mail dir_compliance@domo.vc.

6.3. Utilização de Inteligência Artificial

Os colaboradores da DOMO devem, mandatoriamente, utilizar a inteligência artificial ("A.I.") denominada "Gemini" da Google, por ser a a plataforma oficial do GoogleWorkspace.

É expressamente vedada a utilizaçãode qualquer A.I. (i.e *ChatGPT*, *DeepSeek* e *Perplexity*) em suas versões basicas e/ou gratuítas e/ou *freemium*, para an-alise / revisão / comentários / ajustes, dentre outros, de documentos e/ou arquivos de texto , imagem e/ou vídeo, tendo em vista que tais versões não pagas de A.I. utilizam-se de informações fora do domínio DOMO em suas análises, configurando risco de vazamento de dados.

(**********)