

# **POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO, CIBERSEGURANÇA E LGPD**

Versão Atualizada: 3.0.0 – Setembro/2025

## **POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO, CYBERSEGURANÇA E LGPD**

---

### **Objetivo**

Contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da ENGEFORM GESTAO DE RECURSOS LTDA (“ENGEFORM”), visando garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda. Além disso, estabelecer medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

### **A quem se aplica?**

Esta Política de Confidencialidade, Segurança da Informação, Cibersegurança e LGPD (“Política”) aplica-se a sócios, diretores e funcionários que participem de forma direta das atividades diárias e negócios, representando a ENGEFORM (doravante, “Colaboradores”).

### **Revisão e Atualização**

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, se assim necessário por mudanças legais/regulatórias/autorregulatórias.

### **Responsabilidades**

Os Colaboradores devem atender aos procedimentos estabelecidos nesta Política, informando quaisquer irregularidades ao Diretor de *Compliance* e PLD, que deverá avaliá-las e submetê-las ao Comitê de Compliance e Risco, conforme o caso.

O Diretor de *Compliance* e PLD deve garantir o atendimento a esta Política, sendo o responsável na ENGEFORM por temas de segurança da informação/cibernética, confidencialidade e LGPD.

### **Contexto Operacional e de Negócios**

Esta política foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da ENGEFORM:

- ✓ Todos os sistemas utilizados pela gestora, seja sistemas internos ou de terceiros são acessíveis via *web*;
- ✓ Os fornecedores dos sistemas utilizados pela ENGEFORM se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da ENGEFORM;
- ✓ Os colaboradores da ENGEFORM estabelecem tratativas e formalizam seus entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou e-mail corporativo;
- ✓ A gestora aloca recursos mediante a utilização de corretoras/plataformas de investimento acessíveis pela internet e disponíveis para qualquer dispositivo eletrônico (*laptops, smartphones, tablets* ou computadores de mesa);
- ✓ O sistema de consolidação de carteiras utilizado pela ENGEFORM identifica os clientes por meio de siglas, dispensando a identificação mediante o preenchimento de cadastro com informações pessoais;

- ✓ Os arquivos contendo informações pessoais e financeiras dos clientes da ENGEFORM são armazenados em nuvem, com *backups* periódicos não superiores a 7 (sete) dias corridos, podendo ser recompostos solicitando tais informações aos próprios clientes;
- ✓ Os dispositivos eletrônicos (*laptops, smartphones, tablets*) utilizados no exercício das atividades da ENGEFORM possuem senha de acesso e criptografia;
- ✓ A ENGEFORM utiliza redes sem fio para fornecer acesso à *web* para seus Colaboradores, prestadores de serviço ou visitantes, todas devidamente protegidas por senhas. Em caso de indisponibilidade temporária para acesso à *web*, os Colaboradores utilizam redes/roteadores de redundância;
- ✓ O espaço físico/escritório da ENGEFORM é o local preferencialmente utilizado para as suas atividades, reuniões com clientes, comitês e reuniões comerciais com Colaboradores ou terceiros. Porém, as atividades, rotinas e sistemas da ENGEFORM estão parametrizados para serem passíveis de desempenhados remotamente.

### **Política de Confidencialidade**

São consideradas “Informações Confidenciais” aquelas não disponíveis ao público, que:

- ✓ Identifiquem dados pessoais ou patrimoniais (da ENGEFORM ou de clientes);
- ✓ Sejam objeto de acordo de confidencialidade celebrado com terceiros;
- ✓ Identifiquem ações estratégicas – dos negócios da ENGEFORM, seus clientes ou dos portfólios sob gestão<sup>1</sup>;
- ✓ Abranjam informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da ENGEFORM, e que sejam devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;
- ✓ Sejam assim consideradas em razão de determinação legal, regulamentar e/ou autorregulatória; e que
- ✓ Incluam credenciais de autenticação pessoal do Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás), que sejam de uso pessoal e intransferível.

### **Exceções à Política de Confidencialidade**

Não constitui descumprimento desta Política a divulgação de Informações Confidenciais nos seguintes casos:

- (i) mediante prévia autorização do Diretor de *Compliance* e PLD;
- (ii) em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente; e
- (iii) quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente o Diretor de *Compliance* e PLD acerca da possibilidade de compartilhamento da Informação Confidencial.

### **Identificação, Classificação e Controle da Informação**

O Colaborador que recebe ou prepara uma informação pode, se eventualmente necessário, classificá-la como “Confidencial”. Para tal conclusão, devem ser considerados as questões de natureza legal e

---

<sup>1</sup> Cuja divulgação possa prejudicar a gestão dos negócios, clientes e portfólios a cargo da ENGEFORM, ou reduzir sua vantagem competitiva.

regulatória, de estratégia negocial, os riscos do compartilhamento, as necessidades de restrição de acesso e os impactos no caso de utilização indevida das informações.

Caso haja informação de natureza “Confidencial”, o acesso a mesma deve ser restrito e controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão do Diretor de *Compliance* e PLD, e, quando necessário, da assessoria jurídica da ENGEFORM.

A informação deve receber proteção adequada. Em caso de dúvida, o Colaborador deverá consultar o Diretor de *Compliance* e PLD.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando preferencialmente máquina fragmentadora/trituradora de papéis ou incineradora.

### **Mesa Limpa**

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores, mesmo quando trabalhando remotamente. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

### **Política de Cibersegurança**

Na prestação de seus serviços, a ENGEFORM obtém e lida com informações sensíveis, não disponíveis ao público em geral, e que podem ocasionar perdas irreparáveis em casos de malversação, negligência ou vazamentos<sup>2</sup>.

A ENGEFORM reconhece os principais riscos e ameaças aos seus ativos cibernéticos e adota medidas para preveni-los e mitigá-los. Entre as ameaças mais relevantes estão:

- *Malwares* – *softwares* desenvolvidos para corromper os computadores e redes, como:
  - ✓ vírus: *software* que causa danos às máquinas, redes, *softwares* e bancos de dados;
  - ✓ cavalos de troia: aparecem dentro de outro *software*, criando uma entrada para invasão da máquina;
  - ✓ *spywares*: *software* maliciosos que coletam e monitoram as atividades das máquinas invadidas;
  - ✓ *ransomware*: *softwares* maliciosos que bloqueiam o acesso a sistemas e bases de dados, solicitando resgates para restabelecimento do uso/acesso.
- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como, por exemplo:
  - ✓ *pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - ✓ *phishing*: *links* veiculados por e-mails simulando pessoas ou empresas confiáveis que enviam comunicação eletrônica aparentemente oficial para obter informações confidenciais;
  - ✓ *vishing*: simulação de pessoas ou empresas confiáveis para, por meio de ligações telefônicas, obtenção de informações confidenciais;
  - ✓ *smishing*: simulação de pessoas ou empresas confiáveis para, por meio de mensagens de texto, obtenção de informações confidenciais;
- Ataques a Sistemas e Redes:
  - ✓ ataques de DDOS (*distributed denial of services*): Ações que visam negar ou atrasar o acesso aos serviços ou sistemas da instituição, prejudicando sua operação

<sup>2</sup> Os riscos potenciais relativos a tais dados envolvem invasões, disseminação errônea ou dolosa, acesso indevido e/ou seu roubo/desvio.

- ✓ *botnets* – redes de computadores infectados utilizadas para realizar ataques em larga escala, enviar spam ou propagar vírus;;
- ✓ invasões avançadas (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

O Diretor de Compliance e PLD é o encarregado pela supervisão e mitigação dessas ameaças.

### Gestão de Acessos

A ENGEFORM adota controles rigorosos para gestão de acessos a seus recursos e sistemas:

- Os serviços de rede, internet e e-mail são de propriedade exclusiva da ENGEFORM e devem ser usados moderadamente para fins particulares.
- A ENGEFORM poderá, mediante aprovação do **Diretor de Compliance e PLD**:
  - Monitorar e inspecionar o uso de e-mails, internet e aplicativos;
  - Solicitar justificativas dos usuários pelo uso de recursos;
  - Bloquear acessos ou disponibilizar recursos a terceiros, quando necessário.
- Senhas de acesso serão canceladas imediatamente em caso de desligamento ou transferência de área de um Colaborador.
- Apenas Colaboradores autorizados terão acesso a sistemas, arquivos e pastas, com segregação física e lógica.

### Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e Backups

- Todos os riscos e incidentes de segurança devem ser reportados ao **Diretor de Compliance e PLD**, que adotará as medidas cabíveis.
- O plano de contingência e continuidade de sistemas e serviços fornecidos por terceiros será testado regularmente, e os resultados devem ser compartilhados com a ENGEFORM.
- Em caso de vazamento ou acesso indevido, o **Diretor de Compliance e PLD** deve ser comunicado imediatamente para a tomada de ações corretivas.

### Diretrizes de Cibersegurança

São itens obrigatórios para a instituição:

- Garantir a proteção dos ativos cibernéticos da ENGEFORM, aí incluídos sua rede, sistemas, *softwares*, websites, equipamentos e arquivos eletrônicos.
- Implementar regras para restrição e controle do acesso e privilégios de usuários não pertencentes ao quadro de colaboradores da ENGEFORM;
- Desativar contas de Colaboradores e prestadores de serviço em seu desligamento;
- Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;
- Realizar backups regulares, armazenados em locais seguros e monitorados;
- Monitorar acessos não autorizados e reportar violações ao **Diretor de Compliance e PLD**.

- Realizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário.

São itens OBRIGATÓRIOS de cibersegurança aos Colaboradores:

- Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- Certificar-se da segurança de mensagens e anexos antes de abri-los;
- Ao se ausentar do seu local de trabalho, mesmo quando estiver trabalhando remotamente e mesmo que temporariamente, bloquear a estação de trabalho;
- Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail;
- Utilizar recursos tecnológicos da ENGEFORM somente com a finalidade primordial de atender aos interesses da ENGEFORM<sup>3</sup>.

São itens VEDADOS de cibersegurança aos Colaboradores:

- Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais<sup>4</sup>;
- Divulgar informações confidenciais ou estratégicas sem autorização;
- Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados na rede da ENGEFORM;
- Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/difícultem seu monitoramento pelo Diretor de *Compliance* e PLD;
- Uso de compartilhadores de informações, tais como redes *Peer-toPeer* (P2P – p. ex., Kazaa, eDonkey, eMule, BitTorrent e semelhantes) nas dependências da ENGEFORM.

Exceções de cibersegurança aos Colaboradores:

- Caso haja uso de equipamentos ou dispositivos eletrônicos de propriedade dos colaboradores para desempenhar suas atividades na ENGEFORM, estes se comprometem a adotar as medidas de segurança anteriormente citadas a fim de preservar seus equipamentos e minimizar o risco de comprometimento de segurança às informações sensíveis da ENGEFORM, seus clientes e parceiros de negócio, podendo utilizar tais equipamentos para os diversos fins que considerar pertinentes;
- É facultado ao Diretor de *Compliance* e PLD autorizar exceções à esta política, devendo estar formalizadas por e-mail.

### **Política de Proteção de Dados Pessoais (LGPD)**

A ENGEFORM, no exercício de suas atividades, coleta, armazena e realiza o tratamento de dados pessoais, conforme os parâmetros estabelecidos na Lei n.º 13.709, de 14 de agosto de 2018 (“LGPD”). O tratamento ocorre nos limites estritos e finalidades previstas em lei e nas normas aplicáveis, incluindo, mas não se limitando, às regras da CVM relativas a cadastro e identificação de clientes e operações.

<sup>3</sup> Os computadores, arquivos, e, arquivos de e-mails corporativos poderão ser inspecionados, **independentemente de prévia notificação ao Colaborador**, a fim de disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações.

<sup>4</sup> Sendo proibido, sobretudo, conteúdo pornográfico, racista ou ofensivo à moral e aos princípios éticos.

## Princípios e Finalidades do Tratamento

O tratamento de dados pessoais é realizado com o objetivo de:

- Garantir o cumprimento de obrigações legais e regulatórias aplicáveis às atividades da ENGEFORM;
- Respeitar a estrutura, escala e volume das operações da ENGEFORM, considerando a sensibilidade dos dados tratados;
- Proteger os direitos dos titulares de dados, conforme estabelecido na LGPD e em regulamentações aplicáveis.

Os dados pessoais são coletados e armazenados exclusivamente para os fins acima indicados, sendo absolutamente vedado seu uso para qualquer outra finalidade pela ENGEFORM ou seus Colaboradores. O compartilhamento de dados com reguladores e autoridades será realizado apenas nos limites estritos das normas vigentes e para cumprimento de obrigações legais ou regulatórias.

## Período de Tratamento e Armazenamento

Os dados pessoais serão mantidos pela ENGEFORM:

- Durante o período de vigência do relacionamento com o titular;
- Pelo tempo exigido pelas normas legais ou regulatórias aplicáveis.

Encerrado o período de tratamento, os dados serão eliminados, anonimizados ou tratados conforme previsto na LGPD.

## Direitos dos Titulares de Dados

Os titulares de dados pessoais possuem os seguintes direitos, nos termos do art. 18 da LGPD:

- **Confirmação:** Direito à confirmação da existência do tratamento de seus dados;
- **Acesso:** Direito de acesso aos dados pessoais em posse da ENGEFORM;
- **Correção:** Direito de corrigir dados incompletos, inexatos ou desatualizados;
- **Anonimização, Bloqueio ou Eliminação:** Direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- **Portabilidade:** Direito de transferir os dados pessoais a outro fornecedor, mediante solicitação expressa e conforme regulamentação da autoridade nacional;
- **Eliminação:** Direito de eliminação dos dados pessoais tratados com consentimento, exceto quando:
  - Necessário para cumprimento de obrigação legal ou regulatória;
  - Transferido a terceiros, observando os requisitos legais;
  - Utilizado exclusivamente pela ENGEFORM de forma anonimizada.
- **Informação:** Direito de ser informado sobre:
  - Entidades públicas e privadas com as quais houve compartilhamento de dados;
  - A possibilidade de não fornecer consentimento e as implicações da negativa;
- **Revogação do Consentimento:** Direito de revogar o consentimento previamente concedido.

### Alterações de Finalidade

Caso a ENGEFORM altere a finalidade do tratamento dos dados pessoais para uma finalidade incompatível com o consentimento original, os titulares serão previamente informado e terão o direito de revogar o consentimento, se discordar das alterações.

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; ou
- ✓ determinação da autoridade nacional, quando houver violação ao disposto na LGPD.

### Encerramento do Tratamento de Dados

O tratamento de dados pessoais será encerrado nas seguintes hipóteses:

- Alcance da finalidade para a qual os dados foram coletados ou quando se tornarem desnecessários;
- Conclusão do prazo de tratamento estabelecido;
- Solicitação do titular, incluindo a revogação de consentimento;
- Determinação da autoridade nacional, em caso de violação à LGPD.

### Responsabilidade pela Proteção de Dados

A ENGEFORM mantém disponíveis em seu website os contatos e informações dos responsáveis pela proteção de dados. O **Diretor de Compliance e PLD** é o responsável pela supervisão das práticas relacionadas à LGPD, cabendo a ele:

- Supervisionar os Colaboradores quanto ao cumprimento das diretrizes previstas nesta política;
- Zelar pelo tratamento adequado e seguro dos dados pessoais coletados e tratados pela Gestora;
- Garantir o resguardo dos direitos dos titulares, conforme estabelecido na legislação vigente

### **Testes de Aderência dos Controles**

A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de *Compliance* e PLD e reportados ao Comitê de Compliance e Risco.

Os testes<sup>5</sup> devem verificar se:

- ✓ Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;

---

<sup>5</sup> Que podem ser realizados por terceiros, ou objeto de obrigação contratual, passível de reporte por prestadores de serviço, provedores de dados, aplicativos e ferramentas/*softwares*. Tais conteúdos podem ser passíveis de compor o relatório anual de *Compliance* exigido pela regulamentação aplicável da CVM.

- ✓ Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;
- ✓ Há segregação física e lógica;
- ✓ Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;
- ✓ A manutenção de registros permite a realização de auditorias e inspeções, bem como o cumprimento das obrigações relativas à LGPD.