FOURCE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Código	Versão	Início da vigência
FG-POL004	**01**	**Fevereiro/2026**
Área Emitente		
Diretoria de Compliance e Riscos		
Aprovação		
Diretoria		

Sumário

1. OBJETIVOS

A Fource Gestão de Recursos ("Fource Gestão") reconhece a importância da proteção das informações para garantir a confiança de seus clientes e a conformidade com as exigências regulatórias. Esta Política de Segurança da Informação e Segurança Cibernética ("Política") estabelece diretrizes para preservar a confidencialidade, integridade e disponibilidade dos dados, prevenir riscos cibernéticos e promover uma cultura organizacional voltada à segurança.

Considerando a natureza sensível dos dados tratados, a política estabelece medidas para prevenir, detectar e responder a incidentes de segurança e ameaças cibernéticas, promovendo uma cultura organizacional voltada à gestão de riscos e ao cumprimento das normas regulatórias, como as da Comissão de Valores Mobiliários (CVM) e do Banco Central do Brasil (BCB). Também busca esclarecer responsabilidades e procedimentos para o tratamento adequado das informações, preservando a reputação da empresa e garantindo a continuidade dos negócios.

2. IDENTIFICAÇÃO DE RISCOS (*RISK ASSESSMENT*)

Risk Assessment é definido como o processo de identificação de riscos internos e externos que podem afetar as operações de uma empresa. Neste sentido, a Fource Gestão está exposta a diversos riscos internos e externos que podem afetar suas operações, incluindo:

i. **Dados e Informações:** Risco relacionado à confidencialidade de dados de investidores, clientes, colaboradores, informações operacionais e de ativos sob gestão, além de comunicações internas e externas.;

ii. **Sistemas:** Ameaças e vulnerabilidades em sistemas de tecnologias, sejam estes desenvolvidos internamente ou por terceiros;

iii. **Processos e Controles:** Riscos associados à eficácia dos processos e controles internos;

iv. **Governança e Gestão de Riscos:** Avaliação da eficácia de gestão de riscos da Fource Gestão, incluindo planos de ação, contingência e continuidade de negócios.

Especificamente em segurança cibernética, em conformidade com o Guia de Cibersegurança da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), a Fource Gestão reconhece os seguintes riscos:

i. **Malware:** softwares maliciosos como vírus, cavalo de troia, spyware e ransomware, projetado para danificar, desativar ou obter acesso não autorizado a sistemas de computador. (*Spyware*: Software que permite a um atacante obter informações sobre a atividade de um usuário de computador sem o seu conhecimento; *Ransomware:* Tipo de malware que criptografa os arquivos da vítima e exige um resgate para restaurar o acesso);

ii. **Engenharia Social:** Métodos de manipulação psicológica usados para obter informações confidenciais, incluindo *phishing*, *pharming*, *vishing*, *smishing* e acesso pessoal. (*Phishing:* Tentativa de obter informações confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito, disfarçando-se como uma entidade confiável em uma comunicação eletrônica; *Pharming:* Tipo de fraude online em que o tráfego de um site legítimo é redirecionado para um site falso; *Vishing*: *Phishing* realizado por meio de chamadas telefônicas; *Smishing*: *Phishing* realizado através de mensagens de texto - SMS);

iii. **Ataques de DDoS (Distributed Denial of Service) e Botnets:** Ataques que visam negar ou atrasar o acesso a serviços ou sistemas;

iv. **Invasões (Advanced Persistent Threats - APTs):** Ataques cibernéticos sofisticados que exploram fragilidades específicas no ambiente tecnológico.

2.1. AÇÕES DE PREVENÇÃO E PROTEÇÃO

As medidas de segurança da informação da Fource Gestão visam minimizar as ameaças aos seus negócios. A coordenação e revisão desta Política, incluindo testes e treinamentos, são responsabilidade da Diretoria de Compliance e Riscos.

Para proteger as informações confidenciais da Fource Gestão:

i. É estritamente proibido que colaboradores, provedores de serviços e profissionais terceirizados façam cópias (físicas ou eletrônicas) ou imprimam arquivos da rede Fource Gestão para circulação externa. Exceções devem ser autorizadas por escrito pelo Comitê Compliance e Riscos;

ii. Quando a cópia ou impressão for para fins de negócios da Fource Gestão, o responsável pela posse do arquivo é diretamente encarregado de sua conservação, integridade e confidencialidade;

iii. É proibido o uso de pen-drives, disquetes, fitas, discos ou outros meios que não sejam para uso exclusivo nas atividades da Fource Gestão;

iv. O uso de ativos e sistemas da Fource Gestão (computadores, telefones, internet, e-mail) é prioritariamente profissional. O uso pessoal deve ser evitado e nunca deve ter prioridade sobre o uso profissional;

v. É terminantemente proibido o envio ou repasse por e-mail de material discriminatório, preconceituoso, obsceno, pornográfico, ofensivo ou que possa denegrir a imagem da Fource Gestão;

vi. Colaboradores, provedores de serviços e profissionais terceirizados devem ter bom senso ao receber e-mails e, se possível, evitar mensagens com conteúdo inadequado. Caso recebam, devem apagá-las imediatamente;

vii. A visualização de sites, blogs, fotoblogs, webmails, entre outros, com conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibida.

2.2. GESTÃO DE ACESSOS E EQUIPAMENTOS

2.2.1. Acesso aos Sistemas

O acesso de administrador a áreas de desktop é restrito a usuários aprovados pela Diretoria de Compliance e Riscos, que define os privilégios e níveis de acesso para colaboradores, provedores de serviços e profissionais terceirizados.

A Fource Gestão mantém diferentes níveis de acesso a pastas e arquivos eletrônicos, especialmente aqueles com informações confidenciais, com base nas funções e responsabilidades. O acesso de colaboradores, provedores de serviços e profissionais terceirizados a essas pastas e documentos pode ser monitorado.

2.2.2. Senhas e Logins

As senhas e logins para acesso aos dados nos computadores da Fource Gestão e e-mails remotos são pessoais e intransferíveis, devendo ser mantidas em sigilo por colaboradores, provedores de serviços e profissionais terceirizados.

Para garantir a segurança dos perfis de acesso, as senhas são configuradas de acordo com as regras definidas pelo Comitê de Compliance e Riscos e pela equipe de tecnologia. As senhas devem ser alteradas a cada dois meses.

2.2.3. Uso de Equipamentos e Sistemas

Cada colaborador, provedor de serviços e profissional terceirizado é responsável por manter a segurança das informações armazenadas ou disponíveis nos equipamentos sob sua responsabilidade. Os ativos e sistemas da Fource Gestão, incluindo computadores, telefones, internet e e-mail, são destinados exclusivamente para fins profissionais. O uso pessoal deve ser evitado e nunca deve ter prioridade sobre o uso profissional.

Todos os colaboradores, provedores de serviços e profissionais terceirizados devem ser cuidadosos ao usar seus equipamentos e sistemas, zelando pelo bom uso de todos os recursos. Caso identifiquem má conservação, uso indevido ou inadequado de qualquer ativo ou sistema, devem comunicar imediatamente à Diretoria de Compliance e Riscos.

2.2.4. Acesso Remoto

A Fource Gestão permite o acesso remoto por colaboradores, provedores de serviços e profissionais terceirizados, desde que seja feito sempre mediante o uso de senha para acesso a e-mails e arquivos.

Os colaboradores, provedores de serviços e profissionais terceirizados são instruídos a manter *softwares* de proteção contra *malwares*/vírus em seus dispositivos remotos e a relatar à Diretoria de Compliance e Riscos qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Fource Gestão em ambiente remoto. Informações confidenciais não podem ser armazenadas em dispositivos pessoais.

2.2.5. Monitoramento e Controle de Acesso

O acesso de colaboradores, provedores de serviços e profissionais terceirizados às dependências da Fource Gestão é realizado por meio de crachá de acesso pessoal e intransferível, entregue no momento da contratação.

O acesso à rede de informações eletrônicas utiliza servidores exclusivos da Fource Gestão, que não podem ser compartilhados com outras empresas.

Considerando que o uso de computadores, internet, e-mail e outros dispositivos se destina exclusivamente a fins profissionais, a Fource Gestão monitora a utilização desses meios.

Nesse sentido, a Fource Gestão:

i. Mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos colaboradores, provedores de serviços e profissionais terceirizados, e pode monitorar o acesso a essas pastas e arquivos com base na senha e login disponibilizados;

ii. Pode monitorar o acesso de colaboradores, provedores de serviços e profissionais terceirizados a sites, blogs, fotoblogs, webmails, entre outros, bem como os e-mails enviados e recebidos;

iii. Pode monitorar as ligações telefônicas de seus colaboradores, provedores de serviços e profissionais terceirizados realizadas ou recebidas pelas linhas telefônicas da Fource Gestão para atividade profissional, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação.

2.2.6. Monitoramento e Testes

A Diretoria de Compliance e Riscos (ou pessoa por ele designada) adotará as seguintes medidas para monitorar determinados usos de dados e sistemas, com o objetivo de detectar acessos não autorizados ou outras violações potenciais, com frequência mínima semestral:

i. Monitorar, por amostragem, o acesso de colaboradores, provedores de serviços e profissionais terceirizados a sites blogs, fotoblogs, webmails, entre outros, bem como os e-mails enviados e recebidos;

ii. Monitorar, por amostragem, as ligações telefônicas de seus colaboradores, provedores de serviços e profissionais terceirizados realizadas ou recebidas pelas linhas telefônicas da Fource Gestão para a atividade profissional de cada um, especialmente, mas não se limitando, às ligações da equipe de atendimento da Fource Gestão;

iii. Verificar, por amostragem, as informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, para avaliar a adesão às regras de restrição de acesso e escalonamento.

A Diretoria de Compliance e Riscos poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos previstos nesta Política para avaliar seu cumprimento e eficácia.

3. PLANO DE IDENTIFICAÇÃO E RESPOSTA

3.1. IDENTIFICAÇÃO DE SUSPEITAS

Qualquer suspeita de infecção, acesso não autorizado, comprometimento da rede ou dos dispositivos da Fource Gestão (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer informações confidenciais (mesmo que de forma involuntária), deve ser informada prontamente à Diretoria de Compliance e Riscos. Ela determinará quais membros da administração da Fource Gestão e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

3.2. PROCEDIMENTOS DE RESPOSTA

A Diretoria de Compliance e Riscos solicitará à equipe de tecnologia, por meio de Comitê, explicações sobre qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Fource Gestão, seguindo os critérios abaixo:

i. Avaliação do tipo de incidente ocorrido (por exemplo, infecção por malware, intrusão na rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

ii. Identificação de quais sistemas, se houver, devem ser desconectados ou desabilitados;

iii. Determinação dos papéis e responsabilidades do pessoal apropriado;

iv. Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

v. Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

vi. Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente (por exemplo, em se tratando de informações confidenciais de fundo de investimento sob gestão da Fource Gestão, a fim de garantir a ampla disseminação e tratamento justo da informação confidencial);

vii. Determinação do responsável (ou seja, a Fource Gestão ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Comitê de Compliance e Riscos, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

4. ARQUIVAMENTO DE INFORMAÇÕES

Conforme esta Política, os colaboradores devem arquivar todas as informações, documentos e extratos que possam ser necessários para uma auditoria ou investigação sobre possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro. Essa guarda deve seguir a Resolução CVM nº 21/2021, pelo prazo mínimo de 5 (cinco) anos, ou por um período maior se exigido pela legislação e regulamentação vigentes.

5. PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

A Fource Gestão mantém um Plano de Continuidade de Negócios para evitar interrupções operacionais em situações que impeçam o acesso ao escritório principal.

Todos os dias, os arquivos da rede são automaticamente copiados para um destino na nuvem, com backups feitos instantaneamente.

Além disso, a Fource Gestão utiliza servidores de e-mail externos, permitindo que colaboradores, provedores de serviços e profissionais terceirizados acessem a rede e os e-mails de casa, caso alguma contingência impossibilite o trabalho na sede. Isso garante a continuidade das atividades da Fource Gestão até que a situação seja normalizada.

6. TREINAMENTO

A Diretoria de Compliance e Riscos organizará um treinamento anual dos colaboradores, provedores de serviços e profissionais terceirizados com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de Compliance (descrito na Política de Compliance).

7. PRIVACIDADE

Esta Política se aplica a todas as formas de coleta de dados pessoais que permitem a prestação ou aprimoramento dos serviços da Fource Gestão.

As práticas descritas neste tópico se aplicam ao tratamento de dados pessoais no Brasil e estão sujeitas à legislação aplicável, sobretudo, mas não se limitando à Lei nº 1.709/2018 (Lei Geral de Proteção de Dados).

7.1. COLETA DE DADOS

A coleta de dados começa quando uma contraparte (seja um fornecedor, colaborador ou terceiro) deseja incluir ou atualizar suas informações em nossa base, fornecendo seus dados pessoais. É importante notar que, embora alguns dados sejam fornecidos diretamente pela contraparte, a Fource Gestão também pode coletá-los automaticamente.

Ao aceitar nossas políticas, a contraparte concorda expressamente em fornecer apenas dados pessoais verdadeiros, atuais e precisos, e em não alterar sua identidade ou informações ao acessar e usar os serviços da Fource Gestão. A pessoa que fornece as informações será a única responsável por quaisquer dados falsos, desatualizados ou imprecisos fornecidos à Fource Gestão.

7.2. RETENÇÃO E EXCLUSÃO DE DADOS PESSOAIS

A Fource Gestão garante que durante o período em que a contraparte for um cliente ou colaborador, durante o uso dos nossos serviços e por todo o período em que armazenarmos os seus dados pessoais, eles serão mantidos em ambiente seguro e controlado.

Mesmo após a finalização da utilização de nossos produtos e serviços e quando for autorizado por lei, a Fource Gestão poderá armazenar seus dados pessoais por um período adicional para fins de auditoria, cumprimento de obrigações legais ou regulatórias, para o exercício regular de direito ou ainda pelo prazo necessário de acordo com a base legal que justifique a retenção de dados.

8. DISPOSIÇÕES FINAIS

Todos os colaboradores são responsáveis pelo cumprimento deste documento em complementariedade com o Código de Conduta Ética e com a legislação aplicável vigente. Os superiores imediatos devem garantir que os seus subordinados recebam orientação necessária para atenderem os requisitos deste documento.

Este documento entra em vigor na data de sua publicação, indicada na capa, e deverá ser revisado a cada 24 meses. Em casos de alteração na base legal vigente e/ou mudanças na estrutura organizacional ou operacional da Fource Gestão, os responsáveis poderão, a qualquer momento, iniciar o processo de atualização.

8.1. BASE LEGAL

A Política da Segurança da Informação e Segurança Cibernética da Fource Gestão está fundamentada nas seguintes bases legais e regulatórias:

Comissão de Valores Mobiliários (CVM): A política se alinha aos requisitos dos órgãos reguladores, como a CVM, que fiscaliza o mercado de valores mobiliários no Brasil. Além disso, a Resolução CVM nº 21/2021 é explicitamente mencionada como base para o arquivamento de informações, estabelecendo um prazo mínimo de 5 anos.

Banco Central do Brasil (BCB): A política também considera as normas regulatórias estabelecidas pelo BCB.

Guia de Cibersegurança da ANBIMA: Especificamente no que tange à segurança cibernética, a Fource Gestão está em conformidade com as diretrizes e riscos reconhecidos no Guia de Cibersegurança da ANBIMA.

Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD): As práticas de privacidade e tratamento de dados pessoais descritas na política estão sujeitas à legislação aplicável, "sobretudo, mas não se limitando à LGPD, que regula a coleta, uso, armazenamento e descarte de dados pessoais no Brasil.

8.2. INFORMAÇÕES DE CONTROLE

Versão	Histórico	Data	Responsável
01	Criação do documento	Fevereiro/2026	Diretoria de Compliance e Riscos