



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

JUNHO/2026



SUMÁRIO

1	Apresentação	3
2	Objetivos da Política de Segurança da Informação	3
3	Estrutura	3
4	Segurança da Informação	4
5	Monitoramento e Testes	8
6	Direitos de acesso	8
7	Concessão dos direitos de acesso	9
8	Colaboradores Admitidos	9
9	Desligamento de Colaborador	9
10	Segregação de Atividades	10



1 Apresentação

A Política de Segurança da Informação (“PSI”) da Fox Investimentos Ltda. (“FOX”), aplica-se a todos os Colaboradores e Terceiros que utilizem o ambiente de processamento da FOX, ou acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da FOX tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

Para fins desta Política consideram-se:

- Colaboradores: estagiários, trainees, funcionários, diretores e acionistas;
- Terceiros: prestadores de serviço, clientes e parceiros comerciais.

As diretrizes aqui previstas deverão ser interpretadas de forma integrada com as demais políticas, manuais, códigos e procedimentos internos da Fox Investimentos, especialmente aqueles relacionados à governança corporativa, compliance, gestão de riscos, controles internos, continuidade de negócios, proteção de dados pessoais, confidencialidade, segregação de atividades e prevenção ao uso indevido de informações privilegiadas.

2 Objetivos da Política de Segurança da Informação

A Política de Segurança da Informação da FOX visa proteger as informações de propriedade e/ou sob guarda da FOX, garantindo a disponibilidade, integridade, confidencialidade, legalidade e autenticidade das mesmas.

A Política de Segurança da Informação da FOX visa ainda estabelecer diretrizes a serem seguidas para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, tanto em casos acidentais quanto intencionais.

Também estão sujeitos às disposições desta Política os acessos realizados de forma presencial ou remota, dentro ou fora das dependências da Fox Investimentos, incluindo situações de trabalho remoto, viagens, reuniões externas, uso de redes de terceiros e acesso a sistemas disponibilizados por fornecedores, administradores fiduciários, custodiante, corretoras, plataformas



de investimento ou demais prestadores relevantes ao exercício das atividades da empresa,

3 Estrutura

Atualmente, a FOX desempenha exclusivamente atividades voltadas para a administração de carteiras de títulos e valores mobiliários e fundos de investimento.

As atividades desenvolvidas pela FOX são altamente reguladas, especialmente pela Comissão de Valores Mobiliários, e autorreguladas pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, e consistem basicamente na administração de carteira de títulos e valores mobiliários de seus clientes e de fundos de investimento.

Tais atividades exigem credenciamento específico e estão condicionadas ao cumprimento de uma série de exigências, pré-requisitos e de providências, dentre elas a segregação total de suas atividades de gestão de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas pela FOX ou empresas controladoras, controladas, ligadas ou coligadas.

Neste sentido, a FOX, quando necessário, assegurará aos Colaboradores, seus clientes e às autoridades reguladoras, a completa segregação de suas atividades, adotando procedimentos operacionais adicionalmente àqueles citados em suas Políticas e Códigos, objetivando a segregação física de instalações entre a FOX e empresas responsáveis por diferentes atividades prestadas relativas ao mercado de capitais.

A FOX adotará, quando necessário, vários níveis de segregação efetiva e aferível para atendimento dos objetivos acima mencionados, com a efetiva segregação física das atividades, por meio de instalações separadas, inclusive no que se refere ao acesso a arquivos e documentos (físicos e eletrônicos), ao controle de tais acessos e treinamento dos Colaboradores respectivos.

Todos os equipamentos utilizados pelos Colaboradores são de uso exclusivo da FOX e não poderão ser realocados para outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da FOX, que não poderão ser compartilhados com outras áreas



dentro da própria FOX ou com empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

Somente os colaboradores possuem senha cadastrada de forma a permitir a entrada automática. O acesso de terceiros à FOX somente é permitido, na recepção e na sala de reunião, e somente enquanto acompanhados de pelo menos um colaborador da FOX. O acesso de pessoas estranhas à mesa de operações ou a outras áreas críticas da Gestora, depende de justificativa operacional e obtenção de autorização expressa de um dos Diretores.

Todos os Colaboradores e Terceiros são responsáveis por cumprir esta Política, proteger as informações às quais tenham acesso, utilizar adequadamente os recursos tecnológicos disponibilizados, comunicar imediatamente qualquer suspeita de incidente, vazamento, acesso indevido, perda de informação ou descumprimento das regras aqui estabelecidas.

3.1 Governança da Segurança da Informação

A Fox Investimentos estabelece formalmente uma estrutura de Governança de Segurança da Informação, com o objetivo de assegurar a proteção adequada das informações sob sua responsabilidade, em conformidade com os requisitos legais, regulatórios e com as boas práticas de mercado.

A Alta Administração é responsável por patrocinar, apoiar e supervisionar a Segurança da Informação na Fox Investimentos. Fica designado um Responsável pela Segurança da Informação, incumbido de coordenar a implementação, manutenção e melhoria contínua dos controles de segurança, em conjunto com as áreas de Compliance e Tecnologia da Informação.

Esta Política de Segurança da Informação deverá ser revisada, no mínimo, anualmente ou sempre que houver mudanças relevantes nos processos, no ambiente tecnológico, no arcabouço regulatório ou após a ocorrência de incidentes relevantes de segurança da informação.

4 Segurança da Informação

As medidas de segurança da informação têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da FOX.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede



da FOX e circulam em ambientes externos com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais, conforme descrito no “Termo de Compromisso” e “Termo de Responsabilidade e Confidencialidade”.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da FOX. Nestes casos, o colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais mesmo no ambiente interno da FOX.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação ou leitura, utilizando para tal, uma picotadora.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drives, HD externos, ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Fox Investimentos.

Todas as informações que possibilitem a identificação de um cliente da FOX devem permanecer em arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se for para o atendimento dos interesses da FOX ou do próprio cliente. Tal restrição não se aplica na eventualidade de cumprimento de ordem de autoridade judicial ou administrativa determinando a disponibilização de informações sobre eventual cliente da FOX, cujo atendimento deverá ser previamente comunicado ao coordenador do Comitê de Ética, a quem caberá tomar as providências necessárias.

É proibida a conexão de equipamentos na rede da FOX que não estejam previamente autorizados pelo prestador de serviços de tecnologia e por um dos diretores.



Cada colaborador é responsável por manter o controle sobre a segurança das informações armazenadas e disponibilizadas nos equipamentos que estão sob sua responsabilidade.

4.1 Proteção de Dados Pessoais e LGPD

A Fox Investimentos deverá tratar dados pessoais de clientes, Colaboradores, sócios, prestadores de serviços, parceiros comerciais e demais titulares em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), observando os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, responsabilização e prestação de contas.

O tratamento de dados pessoais deverá ocorrer apenas para finalidades legítimas, específicas e necessárias ao desempenho das atividades da Fox Investimentos, ao cumprimento de obrigações legais, regulatórias e contratuais, à execução de contratos, ao atendimento de solicitações de titulares, à proteção do crédito, ao exercício regular de direitos ou a outras hipóteses legalmente permitidas.

A coleta, armazenamento, utilização, compartilhamento, transmissão e descarte de dados pessoais deverão observar controles adequados de segurança, incluindo restrição de acesso, confidencialidade, rastreabilidade, retenção pelo prazo necessário e descarte seguro. O compartilhamento de dados pessoais com terceiros somente poderá ocorrer quando houver finalidade legítima, base legal adequada, necessidade operacional ou obrigação legal/regulatória, devendo ser observadas cláusulas contratuais de confidencialidade, proteção de dados e segurança da informação.

4.2 Gestão de Riscos de Segurança da Informação

A Fox Investimentos adota um processo formal de Gestão de Riscos de Segurança da Informação, com o objetivo de identificar, analisar, avaliar e tratar riscos que possam afetar a confidencialidade, integridade e disponibilidade das informações. Este processo considera ativos, ameaças, vulnerabilidades, impactos e probabilidades, bem como a definição de planos de tratamento e aceitação de riscos residuais, sob responsabilidade da Alta Administração.

4.2.1. Uso dos ativos e sistemas, Internet e e-mail



A utilização dos ativos e sistemas da FOX, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina a fins profissionais. O uso indiscriminado dos mesmos para fins pessoais deve ser evitado, e nunca deve ser prioridade em relação a qualquer utilização profissional.

A FOX se reserva no direito de gravar qualquer ligação telefônica dos seus colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela FOX para a atividade profissional de cada colaborador, especialmente, mas não se limitando às ligações da equipe de atendimento e da mesa de operação da FOX.

Tendo em vista que a utilização do *e-mail* se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a FOX poderá monitorar toda e qualquer troca, interna ou externa, de *e-mails* dos colaboradores.

A visualização de *sites*, *blogs*, *webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, cor, raça, religião, classe social, opinião política, idade, sexo, preferencial sexual, condição ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também 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 FOX. O recebimento de *e-mails* muitas vezes não depende do próprio Colaborador, mas espera-se o esforço de todos os Colaboradores no sentido de, sempre que possível, evitar receber mensagens com as características descritas previamente nas caixas de *e-mail* disponibilizadas pela FOX.

Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da FOX.

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da FOX, salvo se expressamente autorizado para tanto pelo Comitê de Ética.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum colaborador



identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas, este deve comunicar ao coordenador do Comitê de Ética.

Programas instalados nos computadores, principalmente via Internet (“*downloads*”), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática e pelo Comitê de Ética. Também é proibida a instalação de *software* ilegal (“pirata”) ou que possuam direitos autorais protegidos.

A instalação de novos *softwares*, devidamente licenciados, deve ser comunicada previamente ao responsável pela área de informática e ao coordenador do Comitê de Ética. Estes deverão aprovar ou vetar a instalação e utilização dos *softwares* dos colaboradores para aspectos profissionais e pessoais.

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos *e-mails* que também possam ser acessados via *webmail*, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

Todo conteúdo que está na rede pode ser acessado pelo Responsável pelo Compliance, caso haja necessidade, inclusive *e-mails*. Os demais colaboradores têm acessos previamente definidos na forma abaixo. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais ou administrativas.

É vedada a utilização de ativos da FOX para fins pessoais, não sendo permitido o salvamento de arquivos em qualquer equipamento da Rede.

4.2. 2. Acesso a Rede, Permissões e Senha

Todo usuário, para acessar os dados da rede da FOX, deverá possuir um nome de usuário (“*login*”) e senha, previamente cadastrados pelo Comitê de Ética.

Quem deve fornecer os dados referentes aos direitos de acesso do usuário é o responsável direto pelo usuário, que preencherá um formulário e deverá entregá-la ao Comitê de Ética. Quando da necessidade de cadastramento de um novo usuário para utilização da rede, sistemas ou equipamentos de informática da



FOX, o setor de origem do novo usuário deverá comunicar esta necessidade ao Comitê de Ética, por meio de e-mail, para registro da solicitação, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de TI fará o cadastramento e informará ao usuário qual será a sua primeira senha, que obrigatoriamente será alterada após o primeiro acesso ao sistema, e, posteriormente, a cada 60 (sessenta) dias.

Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho.

4.2.3. Gravação de Ligações e Monitoramento de Internet e E-mail

O conteúdo total de ligações telefônicas e trocas de emails realizados a partir de linhas e/ou sistemas de e-mail, internet, chat e outros disponibilizados pela FOX são de propriedade FOX e devem ser utilizados por todos os colaboradores apenas para o desempenho das suas funções profissionais.

Todas as informações sob responsabilidade da Fox Investimentos deverão ser classificadas de acordo com seu nível de sensibilidade, impacto e criticidade para o negócio. As classificações mínimas adotadas são: Pública, Interna, Confidencial e Restrita.

O tratamento das informações deverá respeitar sua classificação, observando requisitos específicos para armazenamento, acesso, transmissão, compartilhamento e descarte, de modo a prevenir acessos não autorizados, vazamentos ou uso indevido.

Os recursos de infraestrutura de informação da FOX, como *softwares* ou equipamentos, incluindo os computadores da empresa, sistemas de e-mail, internet, chat serão monitorados continuamente, para fins de auditoria e segurança.

Todos os Colaboradores desde já expressamente autorizam, conforme ciência exarada no Termo de Compromisso, a gravação de todas as conversas pelas linhas telefônicas da FOX, bem como a monitoração de todas as comunicações por sistemas de e-mail, internet, chat e etc. para posterior utilização a critério exclusivo da FOX, de forma que a utilização destes recursos para uso pessoal e/ou particular não é encorajado.



Adicionalmente, todos os materiais alocados dentro da FOX, como informações gravadas eletronicamente, ou em papel armazenados em gavetas, mesas, arquivos e outros, incluindo aqueles que eventualmente contenham a marcação de confidencial, pessoal ou privado, são de propriedade da Fox Investimentos.

Por fim, todos os Colaboradores declaram sua expressa anuência para o fato de que a FOX terá acesso, inclusive, a eventuais documentos particulares que tenham sido gerados por meio de ferramentas de trabalho disponibilizados pela empresa.

4.2.4. Backup (Cópia de Segurança dos Dados)

Todos os dados da FOX são protegidos através de rotinas sistemáticas de *backup*. Há cópias criptografadas de todos os dados da FOX em nuvem. A restauração dos dados pode ser efetuada em um novo equipamento com a utilização das mesmas credenciais e chaves de segurança utilizadas na operação de backup.

As rotinas de backup deverão observar periodicidade compatível com a criticidade das informações e sistemas utilizados pela Fox Investimentos, devendo ser mantidas evidências da realização, conclusão e eventual falha dos procedimentos. Os backups deverão ser protegidos contra acesso não autorizado, perda, alteração indevida e indisponibilidade, preferencialmente com uso de criptografia e armazenamento em ambiente seguro.

A restauração dos backups deverá ser testada periodicamente, com o objetivo de verificar a integridade das cópias, a efetividade do procedimento de recuperação e o atendimento aos prazos definidos para retomada das atividades. Falhas identificadas nos testes deverão ser registradas, analisadas e tratadas pela área responsável.

4.2.5. Uso de Antivírus

Todo arquivo em mídia proveniente de entidade externa à FOX deve ser verificado por programas antivírus. Todo arquivo recebido ou obtido através da Internet deve ser verificado por um programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de TI, via rede. O usuário não pode, em



hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

5 Monitoramento e Testes

O acesso de terceiros às informações, sistemas ou ambientes tecnológicos da Fox Investimentos deverá observar critérios mínimos de segurança da informação. Contratos firmados com fornecedores e prestadores de serviços deverão conter cláusulas de confidencialidade, requisitos de segurança, responsabilidades, níveis de serviço e, quando aplicável, direitos de auditoria. A Fox Investimentos deverá manter atividades de monitoramento e testes periódicos dos controles de segurança da informação e segurança cibernética, com o objetivo de avaliar sua efetividade, identificar fragilidades, corrigir deficiências e reduzir riscos operacionais, tecnológicos, regulatórios e reputacionais.

Os testes poderão incluir, conforme aplicável, análise de logs, testes de restauração de backup, avaliação de vulnerabilidades, verificação de atualizações de segurança, simulações de incidentes, testes de phishing, revisão de acessos, avaliação de fornecedores críticos e validação dos procedimentos de continuidade de negócios.

Os resultados dos testes e monitoramentos deverão ser documentados, avaliados pelas áreas responsáveis e, quando relevantes, reportados à Alta Administração, com indicação de falhas identificadas, riscos associados, responsáveis pela correção e prazos para implementação dos planos de ação. Para identificar deficiências no ambiente tecnológico e de segurança cibernética, a FOX faz monitoramento e testes periódicos conforme listados abaixo:

- **Logs**

Os logs dos sistemas são analisados para prevenção de qualquer invasão e anormalidade ocorrida.

- **Auditoria interna de TI**

Na auditoria interna trimestral, testes de disponibilidade dos links de internet, firewall e servidores são realizados para validar backups e redundância.



- **Monitoramento de backup**

As rotinas de backup geram log e fazem o envio por e-mail após a conclusão. As mensagens são verificadas para avaliar a conclusão com êxito da rotina especificada.

- **Monitoramento de tráfego de rede**

Realizado através dos logs nos firewalls de borda. Em cada acesso com suspeita de não autorizado, a conexão é encerrada automaticamente.

6 Direitos de acesso

A Fox Investimentos adotará procedimentos para identificação, avaliação e tratamento de vulnerabilidades em sistemas, aplicações e equipamentos, incluindo a aplicação tempestiva de atualizações e correções de segurança, de acordo com critérios de risco e criticidade.

Através do sistema de diretório Active Directory, são concedidos ou revogados os direitos de acesso dos usuários da rede corporativa.

A revisão aos acessos lógicos é realizada duas vezes por ano, normalmente, nos meses de Janeiro e Julho.

7 Concessão dos direitos de acesso

O Active Directory em conjunto com as diretivas de grupo, gerenciam a concessão de direitos de acesso ao usuário utilizando o conceito de unidades de acesso, que podem ser simples ou compostas. Um exemplo de unidade de acesso simples é o acesso a um determinado diretório da rede. Um exemplo de unidade de acesso composta é o acesso a um determinado sistema, que inclui acesso a diretórios da rede, inclusão do usuário no cadastro de usuários do sistema em questão, acesso aos servidores de bancos de dados, entre outros.

O usuário faz a solicitação de acesso a uma ou mais unidades de acesso via e-mail para o departamento de compliance aprovar juntamente com a gerência da área.

As senhas deverão atender a requisitos mínimos de complexidade, confidencialidade e proteção contra uso indevido, sendo proibido o



compartilhamento entre usuários. Sempre que tecnicamente viável, deverão ser adotados mecanismos adicionais de autenticação para sistemas críticos.

A solicitação é aprovada via e-mail e encaminhada para o suporte de redes que irá conceder o acesso solicitado, conforme autorizado.

Todo usuário criado deverá conter um identificador único.

8 Colaboradores Admitidos

Durante o processo de admissão e contratação de um novo Colaborador, o responsável da área solicitante da contratação, definirá os direitos de acesso necessários que deverão ser concedidos ao Colaborador para que ele possa exercer suas funções em adequação ao seu perfil. As permissões deverão ser validadas pelo Compliance que autorizará o suporte de TI para executar os direitos de acesso. Este processo é formalizado através de e-mail, para fins de registro.

Quando da transferência de colaboradores entre áreas, o responsável pelo suporte realizará um levantamento de todos os recursos de informática utilizados pelo usuário na sua área de origem e informará às gerências de origem e destino do funcionário. As gerências das áreas de origem e destino do funcionário em transferência deverão estabelecer, quais direitos de acesso deverão ser revogados, quais serão mantidos e quais deverão ser criados para que o funcionário possa executar suas novas funções. Este processo é formalizado através de e-mail e aprovado pelo departamento de Compliance.

Se for necessário um período de transição, durante o qual antigos direitos de acesso precisem ser mantidos, tais direitos, bem como a duração do período de transição, devem ser especificados pelas gerências envolvidas. Após o término do período de transição, os direitos de acesso serão sumariamente revogados e comunicados via e-mail.

A Fox Investimentos manterá um processo formal de Gestão de Incidentes de Segurança da Informação, contemplando a identificação, registro, análise, resposta, comunicação e tratamento de incidentes, bem como a adoção de medidas corretivas e preventivas, visando a mitigação de impactos e a melhoria contínua dos controles de segurança.



9 Desligamento de Colaborador

O uso de dispositivos móveis, notebooks e o acesso remoto aos sistemas da Fox Investimentos deverão observar controles mínimos de segurança, incluindo autenticação adequada, proteção dos dispositivos, uso autorizado de redes e preservação da confidencialidade das informações.

No caso de desligamento de Colaborador, será enviado um comunicado ao responsável pelo suporte de TI, que deverá desativar o acesso do funcionário desligado à rede e ao correio eletrônico e aguardará um comunicado para revogação dos direitos deste Colaborador, que deve ocorrer em até 24 horas da ocorrência do desligamento. Antes da exclusão da conta do colaborador, devem ser realizados o backup de todos os arquivos e correio eletrônico.

A Fox Investimentos definirá critérios para geração, retenção, proteção e análise de registros de eventos (logs), de forma a permitir a detecção de incidentes, suporte a auditorias e investigações, bem como o atendimento a requisitos legais e regulatórios.

10 Segregação de Atividades

A FOX reconhece que a segregação de atividades é um requisito essencial para que seja dado o efetivo cumprimento às suas estratégias de administração de recursos de terceiros e às suas Políticas de Investimento Pessoal e de Segurança da Informação.

A FOX adota um conjunto de procedimentos – tais como os definidos no item acima – estabelecidos pelo Comitê de Ética, com o objetivo de proibir e impedir o fluxo de informações privilegiadas e/ou sigilosas para outros departamentos, ou Colaboradores, da instituição que não estejam diretamente envolvidos na atividade de administração de recursos de terceiros.

A eficácia da Segurança da Informação será monitorada por meio de indicadores e métricas, tais como ocorrências de incidentes, resultados de testes, conformidade com treinamentos e revisões de acesso, cujos resultados serão periodicamente reportados à Alta Administração.



Estes procedimentos também buscam impedir que estas informações possam vir a alcançar quaisquer outras empresas, que pertençam ou possam vir a pertencer ao mesmo grupo econômico ou societário que a FOX.

Atualmente, a única e exclusiva atividade exercida pela FOX é a administração de carteiras de títulos e valores mobiliários e a FOX não tem interesse ou expectativa em exercer, no curto e médio prazo, quaisquer outras atividades.

Contudo, caso outras empresas venham a ingressar o grupo econômico da Fox Investimentos ou a FOX futuramente venha a exercer quaisquer outras atividades nos mercados financeiro e de capitais estas atividades deverão ser plena, total e infalivelmente segregadas em todos os níveis, processos administrativos, operacionais e de fluxo de informações, de forma que a higidez e segurança da sua atividade de administração de carteiras de valores mobiliários seja sempre mantida.

Caso a FOX venha a exercer outras atividades nos mercados financeiro e de capitais, o Comitê de Ética definirá, de maneira clara e precisa as práticas que assegurarão o bom, racional e eficaz uso de instalações físicas, equipamentos, arquivos e serviços comuns a mais de um setor da FOX; bem como definirá como proceder-se-á a utilização do espaço físico em sua sede e demais instalações de maneira que as atividades dos diferentes setores da empresa fiquem plenamente segregados antes, durante e após o exercício de suas atividades diárias.

Revisão:

Data de revisão:	Responsável:	Área de ação	Aprovação:
11/06/2026	MCGC	Compliance	