# POLÍTICA DE SEGREGAÇÃO, CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

**Grupo ACE**

24 de Junho de 2024 – Versão 2.0

Ace | Capital

# ÍNDICE

# 1. Introdução e Objetivo

A Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética tem por objetivo descrever os procedimentos observados pelo Grupo ACE para garantir a devida segregação, confidencialidade e segurança das informações, para fins de atendimento ao disposto na regulamentação vigente, incluindo a LGPD, nos termos do Anexo I – Política de Privacidade. Na hipótese de qualquer conflito entre o disposto na Política de Privacidade e o restante da Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética, o disposto na Política de Privacidade deverá prevalecer.

O detalhamento do escopo das atividades de cada uma das Gestoras e regras para mitigação de conflitos de interesse pode ser consultado no Código de Ética e Conduta aplicável às Gestoras.

Esta Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética se aplica a todos os Colaboradores.

Responsáveis: Diretor de Risco, Compliance e PLD.

# 2. Confidencialidade

## 2.1. Procedimentos Gerais

Todas as informações que se referem a sistemas, negócios, estratégias, posições ou a clientes das Gestoras são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na ACE Capital e/ou na ACE Capital Grou e/ou da ACE Capital Saires, conforme o caso, e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação que os Colaboradores tiverem com relação aos clientes das Gestoras deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento do cliente, salvo na hipótese de decisão judicial específica que determine à ACE Capital e/ou à ACE Capital Grou e/ou da ACE Capital Saires, conforme o caso, a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da CVM. Caso a ACE Capital e/ou à ACE Capital Grou e/ou da ACE Capital Saires, conforme o caso, ou qualquer dos Colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser seguido de imediata e expressa comunicação aos clientes afetados, caso não haja legislação ou norma dispondo de forma diversa.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto ao Grupo ACE, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pelas Gestoras. Neste sentido, qualquer conduta suspeita deve ser

informada imediatamente e por escrito à Área de Compliance, para que sejam tomadas as medidas cabíveis.

O Grupo ACE exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da ACE Capital, da ACE Capital Grou e da ACE Capital Saires, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

Todo e qualquer material com informações de clientes ou de suas operações deverá ser mantido nas dependências da Gestora responsável pelo cliente, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do Diretor de Risco, Compliance e PLD. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

A proibição acima referida não se aplica quando as cópias ou impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses do Grupo ACE. 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 prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da ACE Capital, da ACE Capital Grou ou da ACE Capital Saires, conforme o caso.

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, sendo recomendável o seu descarte total.

Colaboradores, quando de sua contratação, devem assinar o Termo de Confidencialidade, presente no Anexo II à Política de Regras, Procedimentos e Descrição dos Controles Internos, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando no Grupo ACE e durante certo período após terem deixado a empresa.

Para fins de manutenção das informações confidenciais, o Grupo ACE exige que seus Colaboradores (i) bloqueiem o computador quando o mesmo não estiver sendo utilizado; (ii) mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro; (iii) descartem materiais usados, destruindo-os fisicamente e (iv) jamais revelem a senha de acesso aos computadores ou sistemas eletrônicos, modificando-as periodicamente.

## 2.2. Vazamento de Informações

Observados os procedimentos específicos relacionado ao vazamento de dados detalhados no item 3.10 do Anexo I e não obstante todos os procedimentos e aparato tecnológico robustos adotados pelo Grupo

ACE para preservar o sigilo das Informações, na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de Risco, Compliance e PLD deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de Risco, Compliance e PLD, primeiramente, identificará se a Informação vazada refere-se ao Fundo ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de Risco, Compliance e PLD procederá da seguinte forma:

1. No caso de vazamento de Informações relativas aos Fundos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao Fundo.

2. No caso de vazamento de Informações relativas aos cotistas:

Neste caso, ao Diretor de Risco, Compliance e PLD procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, o Diretor de Risco, Compliance e PLD ficará à inteira disposição para auxiliar na solução da questão.

# 3. Segurança da Informação

## 3.1. Aspectos Gerais e Procedimentos

Os sistemas de informação, a infraestrutura tecnológica, os arquivos de dados e as informações internas ou externas, são considerados importantes ativos do Grupo ACE.

É necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e que todos os usuários da informação compartilhem da responsabilidade pelos processos de segurança definidos neste documento.

As normas de segurança da informação estabelecem objetivos, funções, ações, mecanismos de delegação e responsabilidades pelos processos, manipulação da informação e controles internos.

Os processos de segurança da informação devem assegurar a integridade, a disponibilidade e a confidencialidade dos ativos de informação do Grupo ACE. Para tanto, o Departamento de TI é incumbido de realizar as seguintes atividades:

- monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;

- orientar os testes da infraestrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;
- assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;
- identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;
- manter a infraestrutura que suporta o ambiente controlado;
- manter a infraestrutura e sistemas atualizados;
- notificar imediatamente os incidentes de segurança ao Diretor de Risco, Compliance e PLD;
- tomar ações, em caso de incidentes de segurança.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (*login* de usuário) em uma periodicidade definida, utilizando modelo de definição de senha de difícil identificação por parte de potenciais *hackers* externos. Tal processo será passivo de auditoria e rastreável eletronicamente baseado no sistema de *login* do servidor e serviços de informação.

Para fins de manutenção da alta disponibilidade do ambiente, foi implantado um *no-break* central para suportar eventuais problemas de energia até a entrada do gerador. O acesso físico ao CPD é controlado e autorizado somente aos membros do Departamento de TI, ao Diretor de Risco, Compliance e PLD e, ao critério deste último, Colaboradores cujo acesso seja considerado essencial.

## 3.2. Segurança de Dados

A segurança de dados se mostra imprescindível à política de segurança da informação adotada pelo Grupo ACE. Desta forma, as regras a seguir são observadas:

- não é permitida a conexão de equipamentos de informática ou software, não pertencentes ao Grupo ACE, na rede corporativa, sem a devida autorização do Diretor de Risco, Compliance e PLD;
- a Área de Compliance e a Área de Risco, podendo solicitar suporte do Departamento de TI, devem efetuar verificações semestrais na rede corporativa, para validar o acesso seguro aos recursos disponíveis. As irregularidades encontradas durante essas verificações devem ser comunicadas ao Diretor de Risco, Compliance e PLD;
- o bloqueio de acesso à rede será efetuado pelo Departamento de TI sempre que solicitado pelo Diretor de Risco, Compliance e PLD, ou caso seja detectado algum risco para a rede ou para os sistemas do Grupo ACE; e

- ♦ todas as máquinas possuem o conector USB bloqueado por *software*, sendo vedada a utilização de *pendrives* ou qualquer dispositivo de transferência de arquivos, sendo concedido acesso restrito ao Diretor de Risco, Compliance e PLD a tais dispositivos.

## 3.3. Backup e Restore de Arquivos

O armazenamento de dados (*backup*) é realizado diariamente em *cloud* e localmente, sendo disponível para *restore* após liberação do responsável de segurança da informação. Para o *backup* das informações do Grupo ACE, estas devem ser armazenadas nos servidores da rede corporativa.

Não haverá garantia de *backup* para arquivos armazenados nas estações de trabalho (*desktops* ou *notebooks*).

O armazenamento em *cloud* ocorre fora do Grupo ACE, sendo periodicamente avaliado.

O *restore* de dados, por sua vez, deve ser solicitado ao Departamento de TI e será realizado de acordo com os procedimentos específicos do mesmo.

## 3.4. Confidencialidade dos Dados

Os usuários devem ter acesso somente às informações necessárias à execução de suas tarefas, sendo de responsabilidade do Departamento de TI, em consonância com a Área de Compliance:

- implementar restrições de acesso aos dados armazenados na rede corporativa, observando as diretrizes constantes deste documento;
- promover destruição dos dispositivos de armazenamento, quando da desativação dos equipamentos; e
- garantir que os controles de segurança, das informações armazenadas em mídias removíveis, estejam de acordo com os critérios definidos neste documento.

A Área de Compliance deve verificar, periodicamente, as informações armazenadas nos dispositivos de armazenamento, estejam eles nos servidores ou nas estações de trabalho, para garantir o armazenamento apenas das informações que são realmente necessárias ao Grupo ACE ou à sua função.

## 3.5. Acesso a Recursos

O acesso a recursos, em síntese, é regido por dois processos:

1. Autenticação:

A autenticação do usuário aos recursos da rede deve ser feita por um *login* e uma senha pessoal, sendo de responsabilidade do Diretor de Risco, Compliance e PLD definir e validar os direitos de acesso.

O usuário, por sua vez, é responsável pela seleção, confidencialidade e troca periódica de sua senha, observando os seguintes aspectos:

- é proibido o compartilhamento de senhas de acesso com outros usuários;

- senhas não devem ser redigidas;
- as senhas devem ser trocadas periodicamente, obedecendo aos prazos controlados sistematicamente, sendo recomendado que não sejam reutilizadas;
- as senhas devem possuir critérios sobre caracteres.

Portanto, não é permitida a criação de *logins* de uso genérico ou compartilhado para os usuários. Compete ao Comitê de Risco, Compliance e PLD definir os quesitos sobre senhas, incluindo: periodicidade mínima de renovação, tipos e quantidade mínima de caracteres, os quais devem ser informados ao Departamento de TI.

2. Monitoramento:

O Departamento de TI é responsável pela implementação, manutenção e atualização dos programas de antivírus nas estações e servidores do Grupo ACE. A atualização dos programas de antivírus nas estações e servidores do Grupo ACE deve ocorrer periodicamente, sempre que estiver disponível uma nova atualização de versão fornecida pelo fabricante do *software* de antivírus.

Todas as estações conectadas à rede corporativa são protegidas com a solução de antivírus determinada, devidamente atualizada. O programa de antivírus proverá serviços como proteção de e-mails, proteção de arquivos, proteção contra *scripts* de internet, monitoramento de acesso de rede (*anti-spy e anti-hacker*) e monitoramento de alteração no registro do sistema operacional.

Assim, o ambiente de rede está preparado para detectar automaticamente eventuais incidências de vírus. Sem prejuízo, os usuários devem informar ao Departamento de TI sobre suspeitas de infecção de vírus.

Não é permitido que os usuários removam, desabilitem ou alterem as configurações dos programas de antivírus.

## 3.6. Internet

O serviço de *internet* corporativo do Grupo ACE foi concebido restrita e exclusivamente como ferramenta de trabalho de pesquisa e tratamento de assuntos relacionados às funções do usuário no Grupo ACE. Portanto, o uso do serviço de *internet* não é autorizado para acesso a *sites web* com conteúdo abusivo, ameaçador, pornográfico, obsceno ou de qualquer outra forma censurável, tampouco para fins comerciais ou ganho pessoal, divergentes da finalidade da ferramenta ou da função do usuário.

O acesso a sites é permitido apenas aos considerados seguros pelo Diretor de Risco, Compliance e PLD e novas liberações deverão ser comunicadas ao Departamento de TI, que fará a liberação no *firewall*, que, conforme a situação fática, poderá ser para todos os usuários, para grupos de usuários ou para um usuário em específico.

O acesso à *internet* não é privativo e poderá ser monitorado quando necessário. A violação das diretrizes acima mencionadas poderá acarretar o bloqueio do serviço, sem aviso prévio, e sanções disciplinares de

acordo com os critérios definidos pelo Comitê de Risco, Compliance e PLD, observado o disposto na Política de Regras, Procedimentos e Descrição dos Controles internos aplicável às Gestoras.

## 3.7. Correio Eletrônico

O correio eletrônico corporativo é um serviço disponibilizado como ferramenta de trabalho e comunicação interna e externa de assuntos relacionados aos negócios do Grupo ACE. Desta forma, o uso do serviço de correio eletrônico não é autorizado para:

- transmissão de material ilegal, difamatório ou que viole a privacidade de terceiros;
- envio de mensagens de conteúdo abusivo, ameaçador, pornográfico, obsceno ou de qualquer outra forma censurável;
- envio de informações do Grupo ACE que infrinjam direitos de propriedade intelectual, sigilo do Grupo ACE ou de terceiros;
- envio de mensagens para informação de senhas ou liberação de acessos para terceiros;
- envio espontâneo de vírus;
- envio de mensagens não solicitadas, tais como piadas, mensagens de autoajuda ou correntes;
- encaminhamento de mensagens do tipo *hoax* (boatos) ou com o conteúdo não comprovado, especialmente mensagens desconhecidas vindas da *internet*;
- envio de mensagens de assuntos políticos;
- fim comercial próprio, divergente da finalidade da ferramenta ou da função do usuário;
- divulgação de informações e campanhas de caráter assistencial e/ou humanitário, sem a devida aprovação do Diretor de Risco, Compliance e PLD.

É expressamente proibido o envio de anexos em mensagens de correio eletrônico, dos tipos:

- jogos;
- *softwares*;
- cartões postais;
- fotos de pornografia;
- músicas (*mp3* e similares).

Na hipótese de envio de mensagens contendo anexo(s) classificado(s) como arquivos proibidos, poderá ocorrer o bloqueio automático de tais mensagens. O bloqueio das mensagens também poderá ser realizado automaticamente caso as mesmas possuam palavras proibidas no campo “Assunto” da mensagem. Compete ao Comitê de Risco, Compliance e PLD definir os tipos de arquivos e relação de palavras proibidas, os quais devem ser informados ao Departamento de TI.

O serviço de correio eletrônico corporativo não é privativo e poderá ser monitorado, acarretando bloqueio do serviço sem prévio aviso, nos casos de violação.

O acesso ao conteúdo das caixas postais é um direito restrito do usuário, porém não exclusivo. O Grupo ACE reserva-se o direito de acesso a estas caixas postais através dos processos de controles internos, conduzidos pela Área de Compliance.

Quando ocorrer a necessidade técnica de manutenção, o acesso ao conteúdo das caixas postais poderá ser efetuado pelo Departamento de TI.

As notificações de férias, viagens a trabalho ou ausência temporária devem ser encaminhadas restritamente às pessoas de relacionamento imediato e/ou interessadas.

A utilização de todo e qualquer e-mail, exceto o regularizado pelo Grupo ACE, é vedada.

## 3.8. Armazenamento de Arquivos na Rede Corporativa

Somente os arquivos de interesse do Grupo ACE poderão ser armazenados na rede corporativa. É proibido o armazenamento de arquivos de conteúdo pornográfico, jogos, filmes, arquivos de áudio e/ou vídeo, *softwares* não autorizados e documentos que não tenham ligações com as atividades profissionais do Grupo ACE, em qualquer recurso da rede corporativa, seja mensagem de correio eletrônico, *drives* de rede ou das estações corporativas.

As informações particulares, com exceção dos itens acima mencionados, poderão ser armazenadas nos *drives* da estação sob a responsabilidade do usuário, cabendo salientar que não é garantido o *backup* ou a restauração de arquivos contidos nas estações de trabalho dos usuários.

A Área de Compliance poderá realizar a exclusão de arquivos armazenados na rede corporativa, se os mesmos não tiverem relação com o negócio do Grupo ACE, tais como músicas (*Mp3, WMA, WAV*, etc.), jogos, imagens *(.gif, .jpg, .bmp*, etc.), *softwares*, pornografia (vídeos, imagens, *softwares*, etc.).

## 3.9. Procedimentos de Segurança Cibernética

Identificação e avaliação de riscos (*Risk Assessment*)

O Grupo ACE deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de *cybercriminals* são os seguintes:

- *malware* (vírus, cavalo de troia, *spyware* e *ransomware*);
- engenharia social;
- *pharming*;
- *phishing scam*;
- *vishing*;
- *smishing*;
- acesso pessoal;
- ataques de DDoS e *botnets*;
- invasões (*advanced persistent threats*).

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, o Grupo ACE definiu todos os ativos relevantes da instituição, fundamentais a seu funcionamento, criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

O Grupo ACE levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

Ações de prevenção e proteção

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados que o Grupo ACE adota, conforme já detalhado neste documento.

O Grupo ACE adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. O Grupo ACE trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de *login* e alteração de senhas são auditáveis e rastreáveis. O Grupo ACE deve criar *logs* e trilhas de auditoria sempre que os sistemas permitam.

O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, à critério do responsável pela segurança cibernética.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, o Grupo ACE deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. O Grupo ACE conta com recursos *anti-malware* em estações e servidores de rede, como anti-virus e *firewalls* pessoais. O Grupo ACE proíbe o acesso a determinados *websites* e a execução de *softwares* e/ou aplicações não autorizadas.

Todo e qualquer material com informações de clientes ou de suas operações deverá ser mantido nas dependências da Gestora responsável pelo cliente, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do Diretor de Risco, Compliance e PLD. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses do Grupo ACE. 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 prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno das Gestoras.

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, sendo recomendável o seu descarte total.

A utilização dos ativos e sistemas pertencentes ao Grupo ACE, incluindo computadores, telefones, *internet*, e-mail e demais aparelhos, se destina a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

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, de modo que estas permaneçam o menor tempo possível nos servidores e computadores do Grupo ACE, bem como avisar prontamente o Diretor de Risco, Compliance e PLD.

Não obstante o disposto no parágrafo anterior, todos os anexos dos e-mails recebidos pelos Colaboradores são rigidamente verificados, de modo que os Colaboradores sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas neste documento.

Dessa forma, o Colaborador pode ser responsabilizado, inclusive, caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

Cada Colaborador é responsável, ainda, por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O Grupo ACE adota também *backup* das informações e dos diversos ativos da instituição, conforme as disposições do presente documento.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com a Res. CVM nº 50, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são caras à prevenção e proteção dos ativos do Grupo ACE e devem ser observadas integralmente.

Pode-se, ademais, realizar testes de invasão externa, *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

Os *logs* e trilhas de auditoria, criados na forma definida no item anterior, podem ser analisados sempre que necessário pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

Por fim, o Diretor de Risco, Compliance e PLD poderá verificar (i) os e-mails repassados pelos Colaboradores, (ii) o modo adotado pelos Colaboradores para utilização dos ativos, sistemas, servidores e rede de informações do Grupo ACE, incluindo a verificação de sites visitados, e (iii) do histórico de acessos às áreas restritas do Grupo ACE.

Plano de resposta

A Área de Compliance e a Área de Risco devem, conjuntamente com o Departamento de TI, possuir um plano formal de resposta a ataques virtuais. No mesmo, o Grupo ACE deve estabelecer os papeis de cada área em tal plano, prevendo o acionamento de Colaboradores-chave e contatos externos relevantes.

O plano de resposta deve levar em conta os cenários de ameaças previstos no *risk assessment*. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

Reciclagem

Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

O Grupo ACE deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

Os Colaboradores deverão participar de treinamentos que abordem o tema da segurança cibernética, os quais serão aplicados pelo responsável pela presente política, em periodicidade não superior a 12 (doze) meses.

## 3.10. Testes Periódicos

O Grupo ACE realizará testes dos seus sistemas de segurança de informações, bem como dos preceitos contidos no presente documento, incluindo, mas não se limitando: procedimentos de descarte de informações pelos Colaboradores e individualização dos usuários.

Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão descritos no relatório anual de controles internos do Grupo ACE e reportados ao Comitê de Risco, Compliance e PLD.

Os testes serão realizados pelo Departamento de TI e buscarão cobrir os seguintes pontos:

- identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de *hardware* e *software*, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;
- estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos do Grupo ACE;

- detecção de possíveis anomalias e/ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;
- criação de um plano de resposta e recuperação de incidentes, que contenha comunicação interna e externa, se necessário. Tal plano será elaborado em conjunto entre a Área de Compliance, Área de Risco e o Departamento de TI, e terá testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de Colaboradores e contatos externos;
- manter o programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas em diretório interno da Área de Compliance.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê de Risco, Compliance e PLD, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

## 4. Segregação de Atividade

Inicialmente, cumpre esclarecer que as Gestoras atuam exclusivamente como administradoras de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais. Em razão disso, não é suscitada qualquer hipótese de conflito no nível de cada uma das Gestoras. Não obstante, as Gestoras manterão a devida segregação entre as suas áreas e implementarão controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

O primeiro nível de segregação refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de gestor, analistas, *compliance*, risco, comercial e administrativo. Perfis de acesso, e o controle são realizados com base nessas divisões.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações poderão ser compartilhadas na base da necessidade (*as-needed basis*) nos comitês e reuniões instituídos pelo Grupo ACE ou pelas Gestoras, sendo que os participantes se responsabilizam pelo sigilo das informações.

O acesso de pessoas que não fazem parte do quadro de Colaboradores será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização do Diretor de Risco, Compliance e PLD, e desde que acompanhadas de Colaboradores. Em caso de antigos Colaboradores, não será permitida a sua permanência nas dependências das Gestoras, com exceção dos casos em que tenha

sido chamado pela área de recursos humanos para conclusão do processo de desligamento, de aposentadoria ou outros. O atendimento a clientes nas dependências das Gestoras deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

As diferentes áreas das Gestoras terão suas estruturas de armazenamento de informações logicamente segregadas das demais, de modo a garantir que apenas os Colaboradores autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações da mesma.

Sem prejuízo, as regras destacadas sobre segurança da informação, tratada neste documento, sobretudo no que tange às segregações eletrônicas e de funções, se aplicam para fins da segregação de atividades e devem ser observadas pelos Colaboradores.

Ademais, o Diretor de Risco, Compliance e PLD possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos administradores ou sócios do Grupo ACE, salvo se for de competência do Comitê de Risco, Compliance e PLD.

Por fim, o Grupo ACE ressalta que os mecanismos de mitigação de conflitos de interesses entre as Gestoras podem ser consultados no Código de Ética e Conduta aplicável ao Grupo ACE.

# 5. Plano de Contingência e Continuidade dos Negócios

## 5.1. Introdução ao BCP

O objetivo do BCP é possibilitar que as Gestoras continuem com as suas operações e serviços essenciais, mesmo nos cenários de crise.

A presente seção define os procedimentos que deverão ser seguidos pelas Gestoras no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais das Gestoras sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

O BCP prevê ações que durem até o retorno à situação normal de funcionamento das Gestoras, dentro do contexto de seu negócio. O seu processo de acionamento se dará pelas pessoas indicadas ao longo da presente política, tão logo haja ciência do cenário(s) de crise(s).

<u>Cenários de Crise</u>

A *Alternative Investment Managment Association* (AIMA) lista em seu documento "*Business Continuity Management for Hedge Fund Managers – version June 2012*" 24 possíveis cenários de crise:

| | | |
|---|---|---|
| 1. Explosão em uma grande área; | 2. Fogo; | 3. Falta localizada de energia; |
| 4. Explosão localizada; | 5. Inundação; | 6. Falha de circuito / terminal; |

| | | |
|---|---|---|
| 7. Explosão na vizinhança; | 8. Pandemia; | 9. Falha de hardware; |
| 10. Bomba radiológica; | 11. Clima extremo; | 12. Vírus / hackers; |
| 13. Guerra ou insurreição civil; | 14. Interrupção de transportes; | 15. Roubo / sabotagem; |
| 16. Alerta de segurança; | 17. Acidentes (dentro ou fora do escritório); | 18. Falha no sinal de telecom (internet e/ou voz); |
| 19. Vazamento de gás; | 20. Eletrocussão; | 21. Falha no hardware de telecom e |
| 22. Terremoto; | 23. Falta geral de energia (apagão); | 24. Falha na rede de celular |

| | |
|---|---|
| ⓘ | **Uma vez que ocorra algum incidente parecido com estes 24 cenários ou algo que chame a atenção do Colaborador, o líder do BCP – que é o Diretor de Risco, Compliance e PLD ou, na ausência deste, o seu *backup* – deverá ser imediatamente comunicado.** |

Desdobramentos

A lista de cenários apresentada acima não tem a pretensão de ser definitiva, existindo, por exemplo, o cenário ocasionado por crises sanitárias e pandemias (vide restrições causadas pelo COVID-19). Além disto, cenários de crise são, por definição, imprevisíveis. No entanto, os cenários acima geralmente levam a combinação de um ou mais dos desdobramentos abaixo:

- perda de acesso ao prédio: significa que todos os Colaboradores que estiverem nos prédios das Gestoras no momento do incidente deverão evacuá-lo e quem estiver fora não poderá entrar;
- perda de pessoal: afeta o *staff* e prestadores de serviços das Gestoras. Inclui ferimentos, doenças, morte e incapacidade de chegar nos escritórios (ou potencialmente trabalhar de casa);
- perda de infraestrutura de TI: inclui falha parcial ou completa da rede de TI, incluindo *hardware* e *softwares* essenciais. O fator-chave é envolver os prestadores de serviços assim que possível para instaurar os sistemas de *backup*;
- perda de infraestrutura de *telecom*: inclui falha parcial ou completa da rede de telecomunicações, incluindo equipamentos, telefones fixos, celulares e a *internet*);
- perda de energia elétrica: falta de energia devido a apagões ou interrupção da rede elétrica devido a chuvas e/ou quedas de árvores.

## 5.2. Introdução ao BCP

Uma vez que o líder do BCP for acionado devido a uma potencial crise, caso seja possível, este convocará (pessoalmente ou via *call-tree*) os colaboradores-chave do Grupo ACE, para tratar especificamente da crise e avaliar conjuntamente a situação e próximos passos.

| | |
|---|---|
| ⓘ | **Na impossibilidade de decisão em conjunto – devido a situação em que a pressão é extrema – o líder do BCP poderá tomar decisões sozinho sobre os próximos passos para gerenciar a crise.** |

Existem geralmente três etapas a serem percorridas após a ocorrência de um evento:

1. gestão da crise;
2. recuperação; e
3. retomada.

Gestão da Crise

1. Etapa Inicial – engloba vários aspectos e decisões fundamentais a serem tomados imediatamente após o incidente:
   1.1. avaliação dos impactos: o foco da reunião do time de crise deve ser em:
      1.1.1. entender o que aconteceu;
      1.1.2. quais são as consequências imediatas e gravidade da situação;
      1.1.3. como manter o *staff* a salvo; e
      1.1.4. o que fazer imediatamente e decidir pela formalização ou não da crise (em caso afirmativo, os próximos passos são seguidos);
   1.2. comunicação ao restante dos Colaboradores;
   1.3. evacuação do prédio afetado de forma coordenada em conjunto com a administração predial;
   1.4. acionar assistência médica imediata, se necessário;
   1.5. notificação dos serviços de emergência (bombeiros, polícia, SAMU), se necessário;
   1.6. condução de chamada para ver os membros do *staff* e visitantes presentes;
   1.7. retomada das tratativas acerca da crise;
   1.8. realocação do *staff*:
      1.8.1. quem vai para casa e quem vai para o *site* de contingência (virtual);
      1.8.2. combinar como serão as próximas comunicações (telefone, mensageria);
   1.9. notificação de parceiros-chave estratégicos: prestadores de serviços de TI e *telecom*; corretoras; e administrador fiduciário dos Fundos;

| | |
|---|---|
| i | **Tomar cuidado para manter a consistência da comunicação ao informar terceiros. Apenas os Colaboradores autorizados a falar em nome da empresa deverão fazer isto.** |

   1.10. iniciar a redundância de TI (caso seja aplicável) em conjunto com o Departamento de TI; e
   1.11. redirecionamento das linhas de telefone para os celulares (caso seja aplicável).

2. Recuperação de Desastre – TI:

Após determinar a necessidade ou não de redundância de TI, o líder do BCP e os colaboradores-chave deverão atuar em conjunto com o Departamento de TI para garantir que qualquer aplicativo e *hardware* críticos continuem a operar via redundância/*backup*. Isto inclui:

- acesso ao servidor e e-mails;

- acesso aos principais servidores (aplicativos e arquivos); e
- acesso remoto aos sistemas.

3. Telecom:

Caso a redundância de *telecom* seja necessária, o provedor deve ser instruído a desviar linhas de dados/e-mail.

4. Comunicação Externa:

A gestão de relacionamentos externos durante uma interrupção das atividades normais é crítica para o curto e médio prazo das Gestoras. No curto prazo, os prestadores de serviços críticos devem ser avisados para que eles adaptem os seus processos para a nova circunstância. No longo prazo, prover uma comunicação clara, pontual e consistente a clientes, distribuidores e contrapartes fortalece a confiança na organização.

O líder do BCP e os colaboradores-chave produzirão um script padrão para comunicar interna e externamente (demais prestadores de serviços, clientes, dentre outros). É muito importante que a comunicação externa seja consistente, uma vez que confusão poderá resultar em perda de confiança.

Caso algum Colaborador (que não esteja autorizado a falar em nome das Gestoras) seja questionado por terceiros, o Colaborador deverá direcionar o terceiro para alguém que esteja autorizado.

<u>Recuperação</u>

A fase de recuperação começa após a crise inicial ter sido contornada, ou seja, o *staff* já foi recolocado, a redundância de TI acionada e terceiros-chave notificados.

A fase de recuperação é composta das subfases a seguir:

1. Comunicação Interna: *call* diário de acompanhamento entre líder do BCP e os colaboradores-chave e outro *call* com os demais Colaboradores. Ambos devem ser minutados pelo líder do BCP e conter os *action points* (atividade/dono/*deadline*).

2. Ações Iniciais de Recuperação:
   2.1. Comitê de Risco, Compliance e PLD: deverá se reunir assim que possível para avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e, caso necessário, tomar as devidas ações;
   2.2. Áreas de Gestão da ACE Capital, Áreas de Gestão da ACE Capital Grou e Áreas de Gestão da ACE Capital Saires: deve ser convocada uma reunião para verificar se todas as informações necessárias ao portfólio das Gestoras estão seguras. Dados faltando ou corrompidos devem ser comunicados ao líder do BCP e os colaboradores-chave. O Diretor de Gestão da ACE Capital, o Diretor de Gestão ACE Capital Grou ou o Diretor de Gestão da ACE Capital Saires, conforme o caso, deverá deliberar se decisões de investimento são requeridas, embora o *trading* discricionário possa ser minimizado, de acordo com as novas condições operacionais aplicáveis às Gestoras;

2.3. Áreas de *Compliance*, Risco e Operações: estes times deverão continuar a manter informados o administrador fiduciário dos fundos sob gestão, corretoras e outros contrapartes operacionais-chave.

3. Cobertura de funções críticas: todas as áreas funcionais deverão ter previamente identificado as suas atividades críticas e o seu pessoal-chave necessário. Estas funções deverão ser conduzidas com qualquer problema sendo escalado ao líder do BCP e os colaboradores-chave.

4. *Data Management*:
   4.1. migração dos trabalhos conduzidos externamente durante a crise para os sistemas essenciais (ou *backup*);
   4.2. *backup* de dados em ambiente de recuperação.

5. Comunicação Externa – *stakeholders*-chave externos devem ser atualizados regularmente.

6. Cenários de Retificação/ Contingência:
   6.1. acesso ao prédio: no caso de o prédio ter sido evacuado, ou o acesso a ele estar negado. É provável que documentos ou *hardware* importantes estejam dentro;
   6.2. buscar acomodação alternativa: no caso de o prédio ter sido gravemente danificado ou destruído e a re-ocupação não seja possível a médio prazo (ou nunca mais).

Retomada

A terceira fase é a transição entre estar trabalhando em "modo recuperação" para voltar ao modo normal (*business as usual*). Deve ser tratada – e gerida – como um projeto, incluindo atividades, *check-lists* e gráficos de Gantt com uma clara linha do tempo.

Os temas cobertos por esta fase são dependentes do evento ocorrido, mas podem incluir:

- Como a organização volta a estar em *compliance* novamente?
- Algum sistema necessita ser reconstruído?
- A ACE Capital e/ou a ACE Capital Grou e/ou a ACE Capital Saires irá mudar para um novo escritório?

## 5.3. Redundâncias e Contingências

Em caso de eventos de crise, as Gestoras possuem contingências e redundâncias de forma a permitir a continuação de suas atividades mesmo em condições adversas.

Redundância de TI / *Backup* de Arquivos

As Gestoras disponibilizam em seus servidores o serviço de *backup* e *restore* de arquivos em *cloud*, que tem o intuito de garantir a segurança das informações, a recuperação em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

Os *backups* são salvos ao longo do dia das pastas de dados de todo o Grupo ACE, incluindo e-mails, devendo ser usado em casos em que não é mais possível a recuperação do arquivo danificado ou perdido.

As Gestoras possibilitam o acesso remoto de todas as mensagens pelos Colaboradores.

O serviço de e-mail das Gestoras é garantido por dispositivo de segurança que executa funções de *firewall* e antivírus no nível do roteador. Além disso, antivírus (*software*) é ativado em cada computador individual na rede de escritório.

Redundância de Infraestrutura (Telecom, Internet e Energia)

Telefonia: o Grupo ACE conta com serviço VOIP de telefone para seus Colaboradores. Em caso de falhas nas linhas telefônicas, os Colaboradores da ACE Capital ainda possuem celulares que podem substituir a telefonia fixa.

Internet: o acesso à internet é disponibilizado por 2 *links* de alta velocidade dedicados e 1 *link* ADSL de 100 mbps.

Energia: em caso de falha de fornecimento de energia, o Grupo ACE possui *no-break* para suportar o funcionamento de seus servidores, rede corporativa, telefonia e estações de trabalho principais (*desktops*) para a efetiva continuidade dos negócios, até que o gerador do prédio no qual está localizado seu escritório seja acionado. Após 30 (trinta) minutos, caso não tenha sido acionado o gerador, ou após 2 (duas) horas, caso não tenha sido reestabelecido o fornecimento de energia, a equipe é deslocada para o trabalho remoto.

Teste de *no-break* realizado duas vezes por ano.

*Site* de Contingência e *Home-Office*

Em caso da perda de acesso a sede das Gestoras, os Colaboradores poderão: (a) acessar o *site* de contingência (ambiente em nuvem) ou (b) trabalhar de casa com acesso VPN (*home-office*).

No *site* de contingência, o Grupo ACE possui 4 (quatro) computadores devidamente configurados em nuvem (máquinas virtuais) cujo acesso é permitido aos colaboradores-chave, englobando, no mínimo, membros das Áreas de Gestão da ACE Capital, Áreas de Gestão da ACE Capital Grou, Áreas de Gestão da ACE Capital Saires, Operações e Risco. Estes computadores possuem a "*software*-padrão" dos aplicativos essenciais das Gestoras para operação e sistemas.

As Gestoras também contam com acesso remoto via VPN à sua rede de dados e alguns aplicativos para os Colaboradores que optarem pelo *home-office*. Tal acesso encontra-se disponível a todos os Colaboradores autorizados pelo Diretor de Risco, Compliance e PLD.

| | |
|---|---|
|  | **As informações dos portfólios, além de estarem nos sistemas internos da ACE Capital, da ACE Capital Grou e da ACE Capital Saires, são disponibilizadas diariamente pelo administrador** |

| | |
|---|---|
| | **fiduciário, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos Fundos.** |

## 5.4. Revisão Anual, Atualização e Testes

Revisão Anual e Atualização

O BCP deverá ser revisado anualmente e atualizado sempre que for necessário. Cada revisão deverá ser aprovada pelo Diretor de Risco, Compliance e PLD e as cópias do plano revisado deverão ser distribuídas a todos os Colaboradores. O BCP também será revisto caso aconteça alguma das situações abaixo:

- mudanças materiais – organizacionais – no negócio das Gestoras;
- mudanças de pessoal;
- mudança de endereço do escritório de uma das Gestoras ou abertura de um escritório adicional;
- introdução de novos processos ou alteração dos existentes;
- *upgrade* ou alterações na infraestrutura de IT e/ou sistemas;
- mudança de prestador de serviço relevante;
- alterações de informações de contatos (p.e., números de telefone).

Testes

O BCP deve ser testado para garantir que o mesmo funcione em caso de necessidade. Diferentes cenários de eventos devem ser testados ao menos anualmente. Os principais testes são elencados a seguir:

- *call tree: o* líder do BCP começará o teste fora do horário comercial - sem aviso prévio - transmitindo uma palavra código para os participantes do *call tree*. No dia seguinte, todos os participantes deverão reportar a palavra-código transmitida. Este teste avalia a viabilidade do *call tree* e se os números de telefone foram corretamente registrados;
- conectividade remota e *site* de contingência: todo o staff que possuir acesso remoto via VPN (*Virtual Private Network*) deverá se logar na rede do Grupo ACE a partir de casa e checar se todos os sistemas essenciais e acessos funcionam perfeitamente. Ao menos um Colaborador das Áreas de Gestão da ACE Capital, um Colaborador das Áreas de Gestão da ACE Capital Grou, um Colaborador das Áreas de Gestão da ACE Capital Saires e um da Área de Risco deverão efetuar os testes através dos computadores (virtuais) localizados no *site* de contingência (virtual);
- redundância de TI: durante um final de semana, Departamento de TI irá acionar o sistema *backup* e todo o *staff* tentará logar no sistema testando as aplicações essenciais. Posteriormente – no mesmo final de semana – o sistema principal/primário será acionado novamente, para testar o processo de retomada;
- redundância de *telecom*: durante um final de semana, todas as linhas fixas de telefone serão testadas e então estes serão testados através de um *call tree* para telefones fixos. Posteriormente – no mesmo final de semana – as linhas fixas serão reativadas e testadas como parte do processo de retomada;

- redundância de energia (*no-breaks*): durante um final de semana, a energia será desligada e o *no-break* interno entrará em funcionamento. Os acessos e os sistemas essenciais deverão ser checados. Posteriormente – no mesmo final de semana – a energia será reativada e os acessos novamente testados como parte do processo de retomada.

Obrigações dos Colaboradores em relação ao BCP

| | |
|---|---|
|  | **O BCP somente funcionará com o devido engajamento de todos os colaboradores-chave do Grupo ACE. Os Colaboradores deverão, obrigatoriamente:**<br>• manter uma versão impressa atualizada do BCP em casa e no escritório;<br>• ter programado no seu celular os números dos telefones do líder do BCP, seus colegas imediatos e do seu supervisor;<br>• testar periodicamente o acesso aos sistemas primários e *backups* via VPN (aqueles que tiverem acesso e estrutura computador/*internet* para o *home-office*) e máquinas virtuais;<br>• manter uma política de mesa limpa (*clean desk policy*): no caso de um roubo ou incêndio, os papéis guardados ficam muito mais seguros do que aqueles deixados soltos;<br>• os Colaboradores que gerenciem ou tenham relacionamentos com prestadores de serviços também devem manter programados os contatos destes no celular. |

## 5.5. Atividades e Responsabilidades Relacionadas ao BCP

Em caso de eventos de crise, as Gestoras possuem contingências e redundâncias, de forma a permitir a continuação de suas atividades mesmo em condições adversas.

Os responsáveis pelas atividades relacionadas ao BCP do Grupo ACE são listados a seguir:

| | |
|---|---|
| Manutenção e atualização do plano | Diretor de Risco, Compliance e PLD |
| Aprovação, revisões e conduzir revisão anual | Diretor de Risco, Compliance e PLD |
| Treinamento e teste anual do plano | Diretor de Risco, Compliance e PLD |
| Implementação do plano em caso de necessidade | líder do BCP e os colaboradores-chave |
| Prover informações do plano para investidores e CVM | Diretor de Risco, Compliance e PLD |
| Revisar BCPs de prestadores de serviços essenciais:<br>• na contratação dos serviços;<br>• na revisão anual do BCP da ACE Capital | Diretor de Risco, Compliance e PLD |

## 6. Sanções Disciplinares

A violação das diretrizes mencionadas neste documento poderá acarretar em sanções disciplinares previstas na Política de Regras, Procedimentos e Descrição dos Controles Internos aplicável às Gestoras.

Em caso de uso indevido, o *login* que fica registrado nos arquivos de *log* do sistema é o do usuário que tem acesso ao correio eletrônico, mesmo que o acesso tenha sido feito por outra pessoa. Somente os usuários liberados é que podem utilizar o acesso. Por esse motivo é extremamente importante que a senha do usuário fique restrita ao seu conhecimento apenas.

O Grupo ACE se reserva o direito de proibir o uso de telefones celulares na área de gestão das Gestoras e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e *internet*, bem como troca de informações escritas transmitidas via *internet*, ou mesmo *intranet*, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes ao Grupo ACE ou utilizados em nome dela, a fim de assegurar o fiel cumprimento desta política de segurança da informação, bem como da legislação em vigor.

## 7. Revisões, Atualizações e Vigência

Esta Política de Segregação, Confidencialidade, Segurança de Informação e Cibernética será revisada sempre que necessário, a fim de aperfeiçoar suas regras ou adequá-las as novas regulamentações. Não obstante as revisões estipuladas, poderá ser alterado sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

Em caso de atualizações, a Área de Compliance informará aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página das Gestoras na rede mundial de computadores.

Esta Política de Segregação, Confidencialidade, Segurança de Informação e Cibernética revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.

## 8. Disposições Gerais

Em cumprimento aos quesitos legais e normativos da LGPD, considerando o teor do Anexo I – Política de Privacidade, a presente política está disponível no endereço eletrônico das Gestoras: www.acecapital.com.br.

# 9. Glossário

**ACE Capital** – significa a ACE Capital Gestora de Recursos Ltda.

**ACE Capital Grou** – significa a ACE Capital Grou Gestora de Recursos Ltda.

**ACE Capital Saires** – significa a ACE Capital Saires Gestora de Recursos Ltda.

**ANBIMA** – Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais.

**ANPD** – Agência Nacional de Proteção de Dados.

**Área de Compliance** – área responsável pelos procedimentos de *compliance* e prevenção à lavagem de dinheiro do Grupo ACE, subordinada ao Diretor de Risco, Compliance e PLD.

**Área de Risco** – área responsável pelos procedimentos de controle de riscos do Grupo ACE, subordinada ao Diretor de Risco, Compliance e PLD.

**Áreas de Gestão da ACE Capital** – significam todas as áreas responsáveis pelos investimentos dos Fundos, subordinadas ao Diretor de Gestão da ACE Capital.

**Áreas de Gestão da ACE Capital Grou** – significam todas as áreas responsáveis pelos investimentos dos Fundos, subordinadas ao Diretor de Gestão da ACE Capital Grou.

**Áreas de Gestão da ACE Capital Saires** – significam todas as áreas responsáveis pelos investimentos dos Fundos, subordinadas ao Diretor de Gestão da ACE Capital Saires.

**Área de Operações** – área responsável pelos procedimentos operacionais, de controle e liquidação, relativos ao Grupo ACE e aos Fundos, não atribuíveis às Áreas de Risco e Compliance, subordinada ao Diretor de Risco, Compliance e PLD.

**BCP** – plano de contingência e continuidade dos negócios.

**Clientes** – significam os cotistas dos Fundos, efetivos ou potenciais, para os quais as condições da Política de Privacidade, sejam aplicáveis.

**Colaborador(es)** – significa sócios, administradores, funcionários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades do Grupo ACE.

**Comitê de Risco, Compliance e PLD** – significa o Comitê de Risco, Compliance e PLD do Grupo ACE.

**CVM** – Comissão de Valores Mobiliários.

**Departamento de TI** – empresa especializada na prestação de serviços de TI, contratada pelo Grupo ACE, subordinada ao Diretor de Risco, Compliance e PLD.

**Diretor de Gestão da ACE Capital** – conforme definido no contrato social da ACE Capital.

**Diretor de Gestão da ACE Capital Grou** – conforme definido no contrato social da ACE Capital Grou.

**Diretor de Gestão da ACE Capital Saires** – conforme definido no contrato social da ACE Capital Saires.

**Diretor de Risco, Compliance e PLD** – conforme definido no contrato social da ACE Capital, da ACE Capital Grou e da ACE Capital Saires.

**Fundo(s)** – fundo(s) de investimentos gerido(s) pela ACE Capital, pela ACE Capital Grou ou pela ACE Capital Saires, conforme o caso.

**Gestora(s)** – significa ACE Capital, ACE Capital Grou ou ACE Capital Saires, quando referidas individualmente, ou ambas, quando referidas em conjunto.

**Grupo ACE** – significa o grupo econômico formado entre a ACE Capital, a ACE Capital Grou e a ACE Capital Saires, em virtude do controle comum exercido pela ACE Capital Partners Participações Ltda, inscrita no CNPJ/ME sob o n° 34.896.561/0001-32.

**Informação(ões)** – toda informação confidencial, reservada ou privilegiada das Gestoras, no contexto da política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética aplicável às Gestoras.

**LGPD** - significa a Lei nº 13.709, de 14 de agosto de 2018, e alterações.

**Política de Regras, Procedimentos e Descrição dos Controles Internos** – significa a Política de Regras, Procedimentos e Descrição dos Controles Internos aplicável às Gestoras, conforme divulgado no endereço eletrônico das Gestoras: www.acecapital.com.br.

**Política de Prevenção e Combate à Lavagem de Dinheiro e Financiamento do Terrorismo (PLDFT) e Cadastro** - significa a Política de Prevenção e Combate à Lavagem de Dinheiro e Financiamento do Terrorismo (PLDFT) e Cadastro aplicável às Gestoras, conforme divulgado no endereço eletrônico das Gestoras: www.acecapital.com.br.

**Política de Privacidade** - significa a Política de Privacidade aplicável às Gestoras, nos termos do Anexo I à presente Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética.

**Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética** – significa a presente Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética aplicável às Gestoras.

**Res. CVM n° 21** - significa a Resolução CVM nº 21, de 25 de fevereiro de 2021.

**Res. CVM n° 50** - significa a Resolução CVM nº 50, de 31 de agosto de 2021.

**Violação** – caracteriza por qualquer ato ou solicitação de ato que: (i) esteja em desacordo com a legislação vigente (leis, normas e/ou regulamentos de autoridades públicas ou órgãos autorreguladores); (ii) esteja

em desacordo com as políticas internas aplicáveis às Gestoras; (iii) seja antiético ou que prejudique de qualquer forma a reputação do Grupo ACE; ou (iv) seja de retaliação a quem tenha reportado à violação.

# ANEXO I – POLÍTICA DE PRIVACIDADE

## Anexo I - 1. Introdução e Objetivo

O objetivo da presente Política de Privacidade aplicável às Gestoras é apresentar os mecanismos utilizados pelas Gestoras para preservar a confidencialidade dos dados pessoais - conforme definido pela LGPD - aos quais as Gestoras eventualmente tiver acesso.

Importante salientar que as Gestoras atuam exclusivamente na qualidade de administradoras de carteiras de valores mobiliários, na categoria "gestor de recursos", nos termos do artigo 1°, §1°, inciso II, da Res. CVM n° 21. Desta forma, esta Política de Privacidade foi desenvolvida considerando o escopo de atuação das Gestoras.

Não obstante, as Gestoras atuam como intermediadoras operacionais de dados cadastrais dos cotistas dos fundos de investimento sob gestão, em virtude da celebração de acordo com o administrador fiduciário e com os distribuidores dos fundos nesse sentido, com o exclusivo objetivo de otimizar a operacionalização do processo de cadastro de cotistas. Neste sentido, caso as Gestoras obtenham acesso aos dados dos Clientes, estes serão arquivados, para fins de cumprimento ao disposto na Res. CVM nº 50 e na Política de Prevenção e Combate à Lavagem de Dinheiro e Financiamento do Terrorismo (PLDFT) e Cadastro aplicável às Gestoras, e submetidos aos processos de segurança descritos nesta Política de Privacidade e na Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética aplicável às Gestoras, no que pese serem dados de manutenção obrigatória, nos termos da legislação em vigor.

## Anexo I - 2. Aspectos Gerais

As Gestoras respeitam a privacidade de todos os titulares de dados pessoais, estando, desta forma, comprometida a tomar todas as medidas possíveis para assegurar de maneira razoável a proteção dos dados pessoais coletados.

Todas as informações são tratadas de acordo com as leis e regulamentações de proteção de dados aplicáveis. Nesse sentido, o tratamento de dados de Clientes é realizado pela Área de Compliance e pelos Colaboradores integrantes da Área de Operações.

As Gestoras declaram, para todos os fins e efeitos de direito, que não recebem dados pessoais considerados sensíveis. São considerados dados sensíveis: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a pessoa natural, na condução das suas atividades.

A privacidade dos dados pessoais das fontes de dados, conforme definido no item “Fontes de Dados” adiante, é de grande relevância para as Gestoras, e temos como política respeitar a confidencialidade da informação e a privacidade.

As Gestoras não são responsáveis pelo uso indevido ou perda dos dados pessoais a que não tem acesso ou controle. As Gestoras também ficam isentas de responsabilidade diante do uso ilegal e não autorizado dessa informação como consequência de uso indevido ou desvio das suas credenciais de acesso, conduta negligente ou maliciosa como consequência de atos ou omissões da sua parte ou de alguém autorizado em seu nome.

# Anexo I - 3. Política de Privacidade

## Anexo I - 3.1. Responsável

Em atenção aos termos da LGPD, o responsável por tratar e resolver questões relacionadas à presente Política de Privacidade será o Diretor de Risco, Compliance e PLD, que conta com o auxílio do Departamento de TI, responsável por implementar as medidas de segurança de informação e proteção de dados pessoais (“DPO”, ou “área responsável”, quando em conjunto com o Departamento de TI). A Área de Compliance é responsável por monitorar e acompanhar as atividades desenvolvidas pelo Departamento de TI, sendo certo que tal departamento responde diretamente ao DPO.

As Gestoras respeitam a privacidade de todos os titulares de dados pessoais, estando, desta forma, comprometida a tomar todas as medidas possíveis para assegurar de maneira razoável a proteção dos dados pessoais coletados.

## Anexo I - 3.2. Fontes de Dados

Conforme mencionado anteriormente, considerando o escopo de atuação das Gestoras (i.e., gestão de recursos de terceiros), identificamos que as fontes de dados centrais são as seguintes:

(i) Colaboradores, incluindo sócios, administradores, diretores, funcionários, estagiários ou consultores;
(ii) Fornecedores;
(iii) Parceiros comerciais; e
(iv) Clientes.

Reiteramos, eventuais dados pessoais compartilhados, sejam de Clientes, fornecedores ou parceiros comerciais, serão armazenas e terão o sigilo assegurado, observados os termos da presente Política de Privacidade, sobretudo o disposto no item “Segurança e Privacidade dos Dados Pessoais”, e da Política de Segregação, Confidencialidade, Segurança da Informação e Cibernética aplicável às Gestoras.

## Anexo I - 3.3. Coleta de Dados Pessoais

Inicialmente, no tocante aos visitantes do website das Gestoras, as Gestoras salientam, para todos os fins, que adotam uma política de não utilizar mecanismos para coletar dados dos usuários que visitam o seu site. Desta forma, não são usadas tecnologias como coleta de localização e endereço IP, através de cookies.

Sendo assim, a coleta de dados pessoais ocorrerá exclusivamente por intermédio das seguintes modalidades:

- E-mail, correio, reuniões, telefone, formulários e contratos, por meio da entrega de documentos e informações pessoais.

Nesses casos, o titular dos dados pessoais prestará as informações com uma das seguintes finalidades: (i) possuir ou pretender possuir relação de trabalho com o Grupo ACE; (ii) fornecer ou pretender fornecer produtos e/ou serviços; ou (iii) solicitar serviços das Gestoras.

- Por meio de fontes publicamente disponíveis.

As Gestoras, sobretudo para garantir a eficiência dos processos de *Know Your Client*, *Know Your Partner* e *Know Your Employee*, poderão realizar consultas sobre dados pessoais em bases públicas.

## Anexo I - 3.4. Dados Pessoais Coletados dos Clientes

Conforme mencionado anteriormente, as Gestoras funcionam como intermediadoras operacionais de dados cadastrais dos cotistas dos fundos de investimento sob gestão, em virtude da celebração de acordo com o administrador fiduciário e com os distribuidores dos fundos nesse sentido, com o exclusivo objetivo de otimizar a operacionalização do processo de cadastro de cotistas. Nesta hipótese, poderão ser coletadas as informações adiante:

I – <u>Se Pessoa Física</u>:

(i) Nome completo;
(ii) Data de nascimento;
(iii) Naturalidade;
(iv) Nacionalidade;
(v) Estado civil;
(vi) Nome da mãe;
(vii) Número do documento de identificação e órgão expedidor;
(viii) Número de inscrição no CPF;
(ix) Nome e respectivo número do CPF do cônjuge ou companheiro, se for o caso*;
(x) Endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP) e número de telefone;
(xi) Endereço eletrônico para correspondência;
(xii) Ocupação profissional;

(xiii) Nome da entidade, com respectiva inscrição no CNPJ, para a qual trabalha, quando aplicável*;

(xiv) Informações atualizadas sobre os rendimentos e a situação patrimonial;

(xv) Informações sobre o perfil do Cliente, conforme regulamentação específica que dispõe sobre dever de verificação da adequação dos produtos, serviços e operações ao perfil do Cliente, quando aplicável;

(xvi) Se o Cliente opera por conta de terceiros, no caso dos administradores de fundos de investimento e de carteiras administradas;

(xvii) Se o Cliente autoriza ou não a transmissão de ordens por procurador*;

(xviii) Endereço completo dos procuradores, se houver, bem como registro se eles são considerados pessoas expostas politicamente ("PEP"), se for o caso, nos termos da Instrução CVM nº 50*;

(xix) Qualificação dos procuradores e descrição de seus poderes, se houver*;

(xx) Datas das atualizações do cadastro;

(xxi) Assinatura do Cliente;

(xxii) Se o Cliente é considerado PEP nos termos da Instrução CVM nº 50;

(xxiii) Cópia dos seguintes documentos: (a) documento de identidade; e (b) comprovante de residência ou domicílio; e

(xxiv) Cópias dos seguintes documentos, se for o caso: (a) procuração; e (b) documento de identidade dos procuradores e respectivo número de inscrição no CPF.

*As informações somente serão exigidas com relação ao cadastro de Clientes que atuem em mercados organizados de valores mobiliários.

II – <u>Se Pessoa Jurídica, exceto pessoas jurídicas com valores mobiliários de sua emissão admitidos à negociação em mercado organizado</u>:

(i) Denominação ou nome empresarial;

(ii) Nomes e CPF dos controladores diretos ou nome empresarial e inscrição no CNPJ dos controladores diretos, com a indicação se eles são PEP;

(iii) Nomes e CPF dos administradores;

(iv) Nomes e CPF dos procuradores, se couber;

(v) Inscrição no CNPJ;

(vi) Endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP);

(vii) Número de telefone;

(viii) Endereço eletrônico para correspondência;

(ix) Informações atualizadas sobre o faturamento médio mensal dos últimos 12 (doze) meses e a respectiva situação patrimonial;

(x) Informações sobre o perfil do Cliente, conforme regulamentação específica que dispõe sobre dever de verificação da adequação dos produtos, serviços e operações ao perfil do Cliente, quando aplicável;

(xi) Denominação ou razão social, bem como respectiva inscrição no CNPJ de pessoas jurídicas controladoras, controladas ou coligadas, quando aplicável, observado que na hipótese de a controladora, controlada ou coligada ter domicílio ou sede no exterior e não ter CNPJ no Brasil, deverá ser informada a razão social e o número de identificação ou de registro em seu país de origem*;

(xii) Se o Cliente opera por conta de terceiros, no caso dos gestores de fundos de investimento e de carteiras administradas;

(xiii) Se o Cliente autoriza ou não a transmissão de ordens por representante ou procurador;

(xiv) Qualificação dos representantes ou procuradores, se couber e descrição de seus poderes;

(xv) Datas das atualizações do cadastro;

(xvi) Assinatura do Cliente;

(xvii) Cópia dos seguintes documentos: (a) documento de constituição da pessoa jurídica devidamente atualizado e registrado no órgão competente; e (b) atos societários que indiquem os administradores da pessoa jurídica, se for o caso;

(xviii) Cópias dos seguintes documentos, se for o caso: (a) procuração; e (b) documento de identidade dos procuradores e respectivo número de inscrição no CPF; e

(xix) Endereço completo dos procuradores, se houver, bem como registro se ele é considerado PEP, se for o caso, nos termos da Res. CVM n° 50*.

*As informações somente serão exigidas com relação ao cadastro de Clientes que atuem em mercados organizados de valores mobiliários.

III – <u>Se Pessoa Jurídica com valores mobiliários de sua emissão admitidos à negociação em mercado organizado</u>:

(i) Denominação ou razão social;

(ii) Nomes e número do CPF de seus administradores;

(iii) Inscrição no CNPJ;

(iv) Endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP);

(v) Número de telefone;

(vi) Endereço eletrônico para correspondência;

(vii) Datas das atualizações do cadastro; e

(viii) Concordância do Cliente com as informações.

IV – <u>Se fundos de investimento registrados na CVM</u>:

(i) A denominação;

(ii) Inscrição no CNPJ;

(iii) Identificação completa do seu administrador fiduciário e do seu gestor, nos termos do inciso II ou III acima, conforme aplicável; e

(iv) Datas das atualizações do cadastro.

V – Nas demais hipóteses:

(i) A identificação completa dos Clientes, nos termos dos incisos I a IV acima, no que couber;

(ii) A identificação completa de seus representantes e administradores, conforme aplicável;

(iii) Informações atualizadas sobre a situação financeira e patrimonial;

(iv) Informações sobre perfil do Cliente, conforme regulamentação específica que dispõe sobre dever de verificação da adequação dos produtos, serviços e operações ao perfil do Cliente, quando aplicável;

(v) Se o Cliente opera por conta de terceiros, no caso dos administradores de fundos de investimento e de carteiras administradas;

(vi) Datas das atualizações do cadastro; e

(vii) Assinatura do Cliente.

VI – No caso de investidores não residentes, o cadastro deve conter, adicionalmente:

(i) Os nomes e respectivos números de CPF das pessoas naturais autorizadas a emitir ordens no Brasil e, conforme o caso, dos administradores da instituição ou responsáveis pela administração da carteira; e

(ii) Os nomes e respectivos números de CPF do representante legal e do responsável pela custódia dos seus valores mobiliários no Brasil.

O tratamento dos dados de Clientes mencionados na presente seção será realizado pela Área de Compliance e pelos Colaboradores integrantes da Área de Operações.

## Anexo I - 3.5. Dados Pessoais Coletados dos Fornecedores e Parceiros Comerciais

As Gestoras coletarão os seguintes dados pessoais de fornecedores e parceiros comerciais:

(i) Dados de identificação e contato dos signatários do contrato, conforme o caso, e principais responsáveis pela empresa;

(ii) Conforme o caso, via do contrato, devidamente assinada por todas as partes, incluindo testemunhas com RG e CPF, contendo a cláusula anticorrupção (pode ser por meio eletrônico ou cópia digitalizada);

(iii) Estabilidade financeira;

(iv) Outros usuários dos serviços do fornecedor ou parceiro comercial; e

(v) Tecnologia e habilidade de entregar os serviços:

## Anexo I - 3.6. Dados Pessoais Coletados de Colaboradores e Candidatos à Vaga de Trabalho na Gestora

As Gestoras poderão, sem se limitar, coletar os seguintes dados pessoais de Colaboradores e Candidatos:

(i) Nome completo, RG, CPF;
(ii) Estado civil;
(iii) Cidade, estado, país, CEP, endereço;
(iv) Telefone, e-mail;
(v) Certificações, conforme o caso;
(vi) Descrever como ficou sabendo da vaga, conforme o caso;
(vii) Informações sobre a graduação: data de término/previsão, instituição, tipo de curso.
(viii) Informações sobre trabalhos anteriores: nome da empresa, data de início, término e cargo ocupado.

## Anexo I - 3.7. Objetivo da Coleta de Dados Pessoais

Em suma, o objetivo da coleta de dados pessoais é garantir a execução das atividades desempenhadas pelas Gestoras e dos fornecedores e parceiros comerciais, bem como manter um canal de comunicação válido e eficaz. Neste sentido, as Gestoras manterão uma relação de fornecedores e parceiros comerciais.

Ademais, a coleta de dados também visa salvaguardar legítimos interesses das Gestoras e dos titulares de dados pessoais, bem como atender aos termos da legislação e regulamentação vigente.

## Anexo I - 3.8. Consentimento por Parte do Titular de Dados Pessoais

Caso a finalidade da coleta para qualquer tratamento de dados pessoais necessite do consentimento do titular de dados pessoais, este será fornecido por meio de instrumento específico (e.g. e-mail válido ou formulário, físico ou eletrônico). As interações realizadas pelas Gestoras com os seus Colaboradores, fornecedores, parceiros comerciais e, eventualmente, Clientes, serão de cunho exclusivamente profissional.

## Anexo I - 3.9. Compartilhamento de Dados Pessoais

Inicialmente, as Gestoras atestam, para todos os fins e efeitos, que não possuem qualquer convênio de informações com outras empresas, tampouco cadastro compartilhado.

As Gestoras somente compartilharão dados específicos com prestadores de serviços cujo acesso seja imprescindível para a consecução do serviço contratado e que se comprometam a manter o nível de cuidado e diligência na manutenção da informação.

Reiteramos, apenas prestadores que necessitem, de forma imprescindível, dos dados e tenham contrato com as Gestoras ou com os veículos de investimento geridos poderão receber os dados específicos necessários para a consecução das atividades. Exemplos de tais prestadores de serviços incluem corretoras e empresas de compensação, empresas de suporte de contabilidade, administradores de fundos, nos termos mencionados anteriormente na presente Política de Privacidade, e escritórios de serviços.

Adicionalmente, as Gestoras poderão compartilhar dados pessoais nos seguintes casos:

(i) Para atendimento à medida necessária dentro dos termos das leis, regras ou regulações aplicáveis;
(ii) Perante a existência de obrigação de divulgação;
(iii) Por legítimo interesse que exija a divulgação; ou
(iv) A pedido expresso do titular de dados, mediante o seu consentimento expresso.

## Anexo I - 3.10. Segurança e Privacidade dos Dados Pessoais

As Gestoras adotam medidas protetivas razoáveis contra ameaças físicas, administrativas e técnicas para proteger suas informações pessoais de acesso, uso e divulgação não autorizados, dentre as quais, além daquelas previstas na Política de Segregação, Confidencialidade, Segurança da Informação e Cibernética aplicável às Gestoras, se destacam as seguintes:

● Proteção de Dados: (i) a Área de Compliance e a Área de Risco, podendo solicitar suporte do Departamento de TI, devem efetuar verificações semestrais na rede corporativa, para validar o acesso seguro aos recursos disponíveis. As irregularidades encontradas durante essas verificações devem ser comunicadas ao Diretor de Risco, Compliance e PLD; (ii) o bloqueio de acesso à rede será efetuado pelo Departamento de TI sempre que solicitado pelo Diretor de Risco, Compliance e PLD, ou caso seja detectado algum risco para a rede ou para os sistemas do Grupo ACE; e (iii) todas as máquinas possuem o conector USB bloqueado por software, sendo vedada a utilização de *pendrives* ou qualquer dispositivo de transferência de arquivos, sendo concedido acesso restrito ao Diretor de Risco, Compliance e PLD a tais dispositivos.

● Confidencialidade dos Dados: os usuários devem ter acesso somente às informações necessárias à execução de suas tarefas, sendo de responsabilidade do Departamento de TI, em consonância com a Área de Compliance: (i) promover destruição dos dispositivos de armazenamento, quando da desativação dos equipamentos; (ii) garantir que os controles de segurança, das informações armazenadas em mídias removíveis, estejam de acordo com os critérios definidos neste documento; e (iii) a Área de Compliance deve verificar, periodicamente, as informações armazenadas nos dispositivos de armazenamento, estejam eles nos servidores ou nas estações de trabalho, para garantir o armazenamento apenas das informações que são realmente necessárias às Gestoras ou às suas funções.

● Controle de Usuário e Acesso Restrito aos Dados Pessoais: para acessar a base de dados e informações nos sistemas do Grupo ACE deverão ser utilizadas somente ferramentas e tecnologias autorizadas e previamente estabelecidas pelo Grupo ACE, de forma a permitir a identificação e rastreamento de quais usuários tiveram acesso a determinadas informações (os logs de acesso ficam armazenados nos sistemas) Acessos a servidores, máquinas, pastas de trabalho e sessões (gestão, comercial, administrativos, etc.) são controlados por logins individuais. Os perfis individuais permitem controle de acesso via função.

● Controle de acesso remoto: as Gestoras contam com acesso remoto via VPN à sua rede de dados e alguns aplicativos para os Colaboradores, quando em regime de *home-office*. Tal acesso encontra-se

disponível a todos os Colaboradores autorizados pelo Diretor de Risco, Compliance e PLD. O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, à critério do responsável pela segurança cibernética.

• Duplo fator: para acessos a sistemas sensíveis, o Grupo ACE exige ainda autenticação de dois fatores para que o acesso se complete. Os sistemas do Grupo ACE são protegidos por *firewall*.

• Armazenamento de dados: o Grupo ACE disponibiliza em seus servidores o serviço de *backup* e *restore* de arquivos em *cloud*, que tem o intuito de garantir a segurança das informações, a recuperação em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados. Os *backups* são salvos ao longo do dia das pastas de dados de toda o Grupo ACE, incluindo e-mails, devendo ser usado em casos em que não é mais possível a recuperação do arquivo danificado ou perdido. Periodicamente, haverá testes de acesso aos sistemas primários e *backups* via VPN (aqueles que tiverem acesso e estrutura computador/internet para o home-office) e máquinas virtuais.

• Inexistência de convênio de informações com outras empresas: conforme mencionado anteriormente, as Gestoras não possuem qualquer convênio de informações com outras empresas, tampouco cadastro compartilhado. As Gestoras somente compartilharão dados específicos com prestadores de serviços cujo acesso seja imprescindível para a consecução do serviço contratado e que se comprometam a manter o nível de cuidado e diligência na manutenção da informação. Reiteramos, apenas prestadores que necessitem, de forma imprescindível, dos dados e tenham contrato com as Gestoras ou com os veículos de investimento geridos poderão receber os dados específicos necessários para a consecução das atividades.

• Termo de Confidencialidade: em relação aos seus Colaboradores e/ou na contratação de terceiros que terão acesso a sistemas, dados e informações consideradas confidenciais, reservadas ou privilegiadas, as Gestoras deverão assegurar-se da existência de cláusula ou termo de confidencialidade NDA em que a parte se comprometa com a não divulgação e manutenção da informação, inclusive destruindo-a caso solicitado pelo Grupo ACE ou após o final do contrato.

Não obstante os robustos processos de proteção de dados adotados pelo Grupo ACE, o Colaborador que detectar possível vazamento deve comunicar imediatamente ao DPO, para que este, no menor prazo possível, diligencie para:

(i) Verificar se o vazamento realmente ocorreu e se teve origem interna ou externa;
(ii) Verificar se medidas protetivas de emergência devem ser tomadas;
(iii) Averiguar se é necessário algum reporte a autoridades policiais;
(iv) Proceder com os devidos reportes aos titulares e às entidades administrativas competentes (incluindo a ANP);
(iv) Analisar eventuais medidas de saneamento e recuperação, inclusive a contratação de empresa especializada, que deverão ser discutidas em conjunto com o Departamento de TI;
(v) Se necessário, recomendar a contratação de advogados especializados na matéria.

Adicionalmente, as Gestoras, conforme o caso, poderá tornar anônimas certas informações pessoais confidenciais.

Por fim, desde a entrada em vigor da LGPD, os contratos celebrados com terceiros, sempre que aplicável, passaram a conter cláusula que versa sobre a proteção de dados. Os Colaboradores, por sua vez, possuem o compromisso formal de aderir e cumprir todas as políticas internas aplicáveis às Gestoras, inclusive a presente Política de Privacidade e a Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética, sendo certo que a violação dos seus termos poderá ensejar na aplicação das penalidades estabelecidas na Política de Regras, Procedimentos e Descrição dos Controles Internos aplicável às Gestoras.

Sem prejuízo dos procedimentos adotados pelas Gestoras para a contratação de terceiros, previstos na Política de Regras, Procedimentos e Descrição dos Controles Internos aplicável às Gestoras, o terceiro a ser contratado deverá demonstrar infraestrutura e processos capazes de tratar os dados pessoais eventualmente recepcionados. Área de Compliance e os Colaboradores integrantes da Área de Operações ficarão responsáveis por manter o monitoramento contínuo periódico acerca do cumprimento, pelo terceiro contratado, da obrigação de tratar os dados pessoais eventualmente recepcionados.

Caso Área de Compliance e/ou os Colaboradores integrantes da Área de Operações identifiquem o descumprimento, pelo terceiro, da obrigação de tratar os dados da forma adequada, o contrato poderá ser rescindido, sem prejuízo das penalidades estipuladas em contrato.

## Anexo I - 3.11. Contato

Conforme mencionado neste documento, possuímos um responsável pela proteção de dados. Caso tenha alguma dúvida sobre como consultar seus dados e exercer seus direitos de titular, nos contate pelo e-mail: compliance@acecapital.com.br. Mediante solicitação dos titulares dos dados, o Grupo ACE procederá com o completo descarte dos mesmos, sendo certo que se reserva o direito de manter as informações exigidas pela regulamentação e legislação em vigor.

## Anexo II – Histórico de Versões

**(A partir de 18/05/2022)**

| **Versão** | **Data de vigência** | **Responsável elaboração** | **Motivos da alteração** | **Responsável aprovação** |
|---|---|---|---|---|
| 1.0 | 18/05/2022 | José Mazzoni | Incorporação da ACE Capital Grou ao Grupo ACE. | Comitê de Risco, Compliance e PLD |
| 2.0 | 24/06/2024 | Simone de Grandis | Incorporação da ACE Capital Saires ao Grupo ACE. | Comitê de Risco, Compliance e PLD |