

AMARY CAPITAL

MANUAL DE SEGURANÇA CIBERNÉTICA E PLANO DE CONTINUIDADE DE NEGÓCIOS 2026

Versão: 2026

Data de aprovação: [30/05/2026]

Área responsável: Risco, Compliance e Controles Internos

Sumário

- 1. Escopo
- 2. Base legal e regulatória
 - 2.1 Interpretação normativa e aplicação prática
- 3. Governança de dados e mitigação de riscos digitais
- 4. Segurança cibernética
 - 4.1 Controles específicos para a gestão de fundos
- 5. Plano de Continuidade de Negócios
 - 5.1 Diretrizes para testes de continuidade de negócios
- 6. Política geral de proteção de dados
- 7. Terceiros críticos e computação em nuvem
- 8. Vigência e atualização
- Anexo I. Matriz de acionamento do PCN
- Anexo II. Registro mínimo de incidentes

1. Escopo

O presente Manual de Segurança Cibernética e Plano de Continuidade de Negócios ("Manual") tem como objetivo identificar, avaliar e mitigar os riscos inerentes às atividades da Amary Capital, na qualidade de gestora de recursos de terceiro, estabelecendo princípios, diretrizes, regras de conduta e procedimentos a serem observados por todas as pessoas que mantenham vínculo com a instituição.

Para fins deste Manual, consideram-se abrangidos os administradores, sócios, diretores, empregados, estagiários, prestadores de serviços, consultores, parceiros e quaisquer terceiros que tenham acesso a sistemas, instalações, informações, dados ou processos da Amary Capital, em razão de cargo, função, posição societária, vínculo empregatício, comercial, profissional, contratual ou de confiança ("Colaboradores ou Associados", individualmente "Colaborador ou Associado").

Este Manual visa assegurar a confidencialidade, a integridade, a disponibilidade e a rastreabilidade das informações obtidas ou produzidas no exercício das atividades da Amary Capital, incluindo informações relacionadas às carteiras dos fundos sob gestão, ordens, posições, estratégias, relatórios de risco, comunicações internas e externas, documentos regulatórios, dados pessoais e demais ativos informacionais.

As medidas previstas neste documento podem ser acionadas total ou parcialmente, em qualquer etapa, sempre que necessário para resposta a incidentes de segurança, indisponibilidade de sistemas, falhas operacionais, eventos externos, incidentes com terceiros críticos ou situações que representem risco à continuidade das operações da Gestora.

Adicionalmente, este Manual estabelece procedimentos preventivos e operacionais relacionados ao Plano de Continuidade de Negócios ("PCN"), com o objetivo de garantir a continuidade das atividades críticas da Amary Capital, especialmente gestão de carteiras, tomada de decisão de investimento, roteamento e acompanhamento de ordens, controles de risco, enquadramento, conciliação, comunicação com administradores fiduciários, custodiantes, corretoras, distribuidores e demais prestadores relevantes.

O Manual será disponibilizado aos Colaboradores e Associados da Amary Capital por meio dos canais internos da instituição. Sempre que houver atualizações, as versões revisadas deverão ser comunicadas aos envolvidos e, quando requerido, disponibilizadas aos órgãos reguladores e autorreguladores aplicáveis.

2. Base legal e regulatória

O presente Manual foi elaborado em conformidade com as disposições legais e regulatórias aplicáveis às atividades da Amary Capital, em especial:

1. Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21"), que disciplina o exercício profissional de administração de carteiras de valores mobiliários;
2. Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM 175"), que dispõe sobre a constituição, o funcionamento e a divulgação de informações dos fundos de investimento, bem como sobre a prestação de serviços aos fundos;
3. Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de Administração e Gestão de Recursos de Terceiros, bem como suas Regras e Procedimentos aplicáveis;
4. Lei nº 13.709, de 14 de agosto de 2018, conforme alterada, conhecida como Lei Geral de Proteção de Dados Pessoais ("LGPD");
5. Guias, questionários, orientações e boas práticas da ANBIMA relacionados à contratação de terceiros, serviços de computação em nuvem, segurança cibernética, risco de liquidez e gestão de recursos de terceiros;
6. Demais normas, orientações, manifestações, ofícios e comunicados emitidos pelos órgãos reguladores e autorreguladores aplicáveis às atividades da Gestora.

2.1 Interpretação normativa e aplicação prática

Para fins de interpretação deste Manual, os termos aqui utilizados terão o significado atribuído pela regulamentação aplicável, especialmente pela Resolução CVM 175, quando pertinente. As referências a Fundos de Investimento incluem suas respectivas Classes e Subclasses, quando existentes, e as referências a Regulamento abrangem anexos, apêndices e demais documentos complementares.

A aplicação prática deste Manual deve observar o porte, o perfil de risco, a estrutura operacional, a natureza dos fundos sob gestão, o nível de dependência de terceiros críticos e a complexidade dos sistemas utilizados pela Amary Capital. Em caso de conflito entre este Manual e norma legal ou regulatória superveniente, prevalecerá a norma vigente, devendo o Manual ser atualizado no menor prazo razoável.

A Amary Capital, como gestora de recursos, não substitui as obrigações próprias do administrador fiduciário, custodiante, escriturador, distribuidor ou demais prestadores de serviços dos fundos. Contudo, deve manter controles suficientes para gerir seus próprios riscos operacionais, tecnológicos, cibernéticos e de continuidade, bem como avaliar, acompanhar e escalar eventos envolvendo terceiros críticos que possam afetar a gestão dos fundos.

3. Governança de dados e mitigação de riscos digitais

Risco pode ser definido como a possibilidade de ocorrência de perdas decorrentes de falhas, deficiências ou inadequações em processos internos, sistemas de informação, controles operacionais, condutas humanas, terceiros ou eventos externos que possam comprometer a segurança, a integridade, a disponibilidade, a confidencialidade ou a rastreabilidade das informações e operações da Amary Capital.

No contexto de fundos geridos, a materialização de riscos digitais pode afetar a capacidade de acessar plataformas de negociação, consultar posições e preços, validar enquadramento, executar ordens, monitorar riscos de mercado e liquidez, realizar reconciliações, enviar informações a prestadores de serviços e cumprir prazos regulatórios ou contratuais.

A Amary Capital identifica, monitora e busca mitigar riscos internos e externos relacionados à segurança da informação, com especial atenção aos seguintes elementos:

- **Dados e informações:** informações confidenciais ou estratégicas relativas a fundos, classes, subclasses, carteiras, ativos, posições, ordens, limites, preços, modelos, relatórios de risco, estratégias de investimento, comunicações internas e externas, documentos regulatórios e dados pessoais de investidores, cotistas, clientes, Colaboradores e Associados, quando acessados pela Gestora.
- **Sistemas:** infraestrutura tecnológica, ambientes em nuvem, e-mail corporativo, repositórios de documentos, sistemas de gestão de carteira, plataformas de negociação e roteamento de ordens, sistemas de risco, provedores de dados de mercado, APIs, portais de administradores fiduciários, custodiantes, corretoras e demais prestadores.
- **Processos e controles:** rotinas de gestão, análise, trading, pré e pós-negociação, controle de enquadramento, batimento de carteira, conciliação, validação de informações, comunicação com terceiros, registro de evidências, aprovação de acessos, resposta a incidentes e supervisão de controles.
- **Governança da gestão de riscos:** estrutura, papéis, responsabilidades, instâncias de reporte e mecanismos de acompanhamento adotados para identificar, avaliar, monitorar, controlar, mitigar e comunicar riscos operacionais, tecnológicos e cibernéticos.

AMARY CAPITAL

As consequências práticas decorrentes de riscos são mitigadas por meio do cumprimento das políticas, normas e manuais internos da Amary Capital, bem como da atuação coordenada entre Diretoria, Compliance, Controles Internos, Risco, Tecnologia da Informação e demais áreas envolvidas nas atividades de gestão de recursos.

A área de Tecnologia da Informação, interna ou terceirizada, atuará sob coordenação da administração da Amary Capital e com apoio de Compliance e Controles Internos. Quando serviços de TI forem prestados por terceiros, a Amary Capital manterá supervisão compatível com a criticidade dos serviços e com o acesso concedido a dados, sistemas e ambientes.

Todos os Colaboradores e Associados devem estar devidamente capacitados e conscientes de suas responsabilidades na prevenção e no gerenciamento de riscos, contribuindo ativamente para a identificação, reporte e mitigação de eventuais vulnerabilidades ou incidentes.

O gerenciamento de riscos ocorre por meio de um conjunto estruturado de atividades, controles e processos. Entre essas atividades destacam-se:

- realização de treinamentos periódicos de segurança da informação, proteção de dados e continuidade de negócios;
- identificação conjunta de riscos, fragilidades e vulnerabilidades em processos, sistemas e terceiros críticos;
- categorização e avaliação de riscos de acordo com impacto, probabilidade, criticidade, urgência e relação com operações críticas;
- execução de testes periódicos de controles, acessos, backups, restauração, resposta a incidentes e continuidade;
- elaboração, aprovação, comunicação e acompanhamento de planos de ação, com prazos, responsáveis e evidências;
- revisão periódica de perfis de acesso, usuários privilegiados, chaves de API e permissões em sistemas críticos;
- registro e reporte de incidentes operacionais, tecnológicos e cibernéticos ao Comitê de Compliance, Diretoria ou instância equivalente, quando aplicável.

As principais medidas de controle interno adotadas pela Amary Capital para prevenção de riscos operacionais e tecnológicos incluem:

- controle de acesso com autenticação multifator, princípio do menor privilégio e segregação de funções;
- confirmação, reconciliação e validação de ordens enviadas a corretoras, contrapartes, plataformas de negociação e demais intermediários;

- validação de negócios realizados, incluindo conferência de dados em sistemas internos, relatórios de execução, notas de corretagem, arquivos de administradores e extratos de custodiantes;
- reconciliação periódica de posições, caixa, movimentações e eventos, de acordo com a criticidade de cada fundo e com os prazos operacionais aplicáveis;
- monitoramento de enquadramento, limites, liquidez, exposição a fatores de risco e eventuais alertas de sistemas de risco ou prestadores;
- acesso remoto controlado aos sistemas de gestão, trading, risco, informação e documentos, mediante mecanismos de segurança, criptografia e autenticação apropriados;
- registro, investigação e reporte de incidentes operacionais e tecnológicos, com objetivo de monitorar falhas de processo e promover melhoria contínua.

4. Segurança cibernética

No que se refere especificamente à segurança cibernética, a Amary Capital identifica as principais ameaças em linha com boas práticas de mercado, guias de autorregulação aplicáveis e características do seu modelo operacional de gestora de fundos.

- **Malware e ransomware:** softwares desenvolvidos para comprometer computadores, sistemas, redes ou dados, incluindo vírus, cavalos de Troia, spyware e ransomware, que podem resultar em perda, alteração, sequestro ou indisponibilidade de dados e sistemas.
- **Engenharia social:** métodos de manipulação utilizados para induzir usuários a fornecer credenciais, aprovar transações, abrir arquivos maliciosos ou realizar ações que comprometam a segurança, incluindo phishing, vishing, smishing, pharming e acesso pessoal indevido.
- **Ataques de DDoS e botnets:** ataques voltados a negar, degradar ou atrasar o acesso a serviços, sistemas, portais, redes e plataformas, comprometendo a disponibilidade das operações da Gestora.
- **Invasões e ameaças persistentes avançadas:** ataques realizados por agentes sofisticados que utilizam técnicas avançadas para identificar e explorar vulnerabilidades específicas em ambientes tecnológicos.
- **Comprometimento de credenciais:** uso indevido de senhas, tokens, chaves de API, dispositivos, contas privilegiadas ou sessões ativas para acessar sistemas críticos, executar ordens, alterar dados ou extrair informações.
- **Vazamento ou exposição indevida de dados:** perda de confidencialidade decorrente de compartilhamento indevido, configuração inadequada de nuvem, envio incorreto de arquivos, permissões excessivas ou uso de canais não autorizados.

- **Riscos de terceiros e integrações:** falhas em provedores de tecnologia, plataformas de mercado, administradores, custodiantes, corretoras, provedores de dados, APIs e serviços de nuvem que possam afetar disponibilidade, integridade ou confidencialidade das operações.

Com base na identificação dessas ameaças, a Amary Capital avalia e define continuamente planos estratégicos de prevenção, monitoramento, detecção e resposta a incidentes, visando à mitigação ou eliminação dos riscos identificados. Esses planos contemplam ajustes nos controles de segurança, procedimentos de recuperação e retomada das atividades normais, bem como a preservação de evidências para investigação.

As medidas de segurança da informação adotadas pela Amary Capital têm como objetivo minimizar ameaças aos seus negócios e assegurar o cumprimento deste Manual, buscando principalmente a proteção de informações confidenciais, a integridade dos dados, a disponibilidade dos sistemas, a rastreabilidade das atividades e a continuidade das operações de gestão dos fundos.

As instalações físicas da Amary Capital devem ser protegidas por controles de acesso apropriados, com o objetivo de assegurar a segurança de Colaboradores e Associados, preservar o sigilo das informações e reduzir riscos de acesso não autorizado a ativos físicos ou documentos. Em regime de trabalho remoto ou híbrido, as diretrizes de segurança aplicam-se igualmente aos ambientes de acesso externo.

Todos os equipamentos conectados aos ambientes corporativos da Amary Capital devem possuir acesso restrito, mecanismos de proteção e configuração de segurança compatível com sua criticidade. Computadores e dispositivos utilizados por Colaboradores e Associados devem permanecer protegidos, atualizados e configurados de acordo com os padrões estabelecidos pela Gestora. Sempre que um computador for deixado sem supervisão, a sessão deve ser bloqueada pelo responsável.

Todos os sistemas que contenham informações sensíveis ou críticas devem exigir autenticação multifator como requisito mínimo de segurança, sempre que tecnicamente disponível. O acesso aos sistemas será concedido de acordo com o princípio do menor privilégio, sendo restrito às permissões necessárias para o desempenho das funções do usuário. Perfis de acesso a sistemas críticos devem ser revisados, no mínimo, trimestralmente ou sempre que houver alteração de função, desligamento, mudança relevante de escopo ou indício de uso indevido.

As ações realizadas em sistemas críticos, incluindo plataformas de negociação, sistemas de risco, repositórios de dados, e-mail corporativo e portais de terceiros, devem ser registradas e auditadas, na medida em que os sistemas permitirem, garantindo rastreabilidade e suporte aos processos de investigação e resposta a incidentes.

AMARY CAPITAL

A Amary Capital mantém estrutura de resposta a incidentes de segurança da informação. Em caso de incidentes relevantes envolvendo dados pessoais, informações críticas, continuidade operacional ou integridade das operações de gestão, poderá ser realizada notificação às autoridades competentes, tais como ANPD, CVM e ANBIMA, bem como aos clientes, fundos, administradores fiduciários ou demais partes afetadas, quando aplicável, de acordo com a legislação vigente, regulamentos dos fundos, contratos e políticas internas.

Nessas situações, deverá ser conduzida análise pós-incidente, com elaboração de relatório contendo identificação das causas, impactos, medidas adotadas, responsáveis, prazos, evidências e medidas corretivas necessárias, as quais deverão ser implementadas no menor prazo possível para mitigar a recorrência do evento.

4.1 Controles específicos para a gestão de fundos

Considerando a natureza dos fundos geridos, a Amary Capital deve preservar a capacidade de acompanhamento dos mercados, tomada de decisão de investimento, roteamento e acompanhamento de ordens, validação de limites, comunicação com prestadores e registro de evidências mesmo em cenários de contingência. Para esse fim, os controles mínimos abaixo devem ser observados:

Processo crítico	Controle esperado	Responsável primário
Gestão e trading	MFA, credenciais individuais, logs, segregação de usuários, canal alternativo com corretoras, validação de ordens e acompanhamento de execução.	Gestão / Mesa
Risco e enquadramento	Acesso seguro a posições, limites, relatórios de risco, preços e alertas; registro de exceções e escalonamento de desenquadramentos.	Risco / Gestão
Back office e middle office	Conciliação de posições, caixa, operações e arquivos de administradores, custodiantes e corretoras; trilha de auditoria dos batimentos.	Operacional
Dados de mercado	Fontes alternativas de consulta para preços, curvas, indicadores, índices e informações necessárias à decisão de investimento.	Gestão / Risco
Comunicação crítica	Canais corporativos seguros e contatos de contingência para	Compliance /

Processo crítico	Controle esperado	Responsável primário
	administradores, custodiantes, corretoras, distribuidores, provedores e reguladores.	Operacional
Documentos e evidências	Armazenamento em repositório corporativo, controle de versões, permissões por função, backups e retenção compatível com políticas internas.	Compliance / TI

A execução direta das atividades de segurança da informação e segurança cibernética é de responsabilidade da área de Tecnologia da Informação, interna ou terceirizada, que atuará com apoio de Compliance, Controles Internos, Risco e Diretoria. Compete a essas áreas, entre outras atribuições:

- realizar monitoramento contínuo da infraestrutura tecnológica e dos sistemas críticos, conforme disponibilidade e contratos aplicáveis;
- conduzir ou coordenar testes periódicos de segurança, backups, restauração e continuidade;
- promover treinamentos e conscientização dos Colaboradores e Associados;
- revisar e atualizar periodicamente este Manual e os procedimentos relacionados;
- analisar incidentes e implementar medidas de mitigação;
- realizar simulações de cenários de ameaças cibernéticas ou indisponibilidade operacional, quando aplicável;
- avaliar periodicamente prestadores de serviços críticos, incluindo provedores de nuvem, tecnologia, plataformas de negociação, dados e sistemas.

5. Plano de Continuidade de Negócios

A Amary Capital adota arquitetura tecnológica baseada predominantemente em ambientes digitais e serviços de computação em nuvem, utilizando provedores e ferramentas que devem atender a padrões adequados de segurança, resiliência e disponibilidade. A Gestora deve manter processos de avaliação e acompanhamento de terceiros críticos, observando sua relevância para as atividades de gestão, risco, trading, documentação, comunicação e controles internos.

Com o objetivo de garantir a confidencialidade, integridade e disponibilidade das informações, o tráfego de dados deve ocorrer por meio de conexões seguras e criptografadas, incluindo o uso de redes privadas virtuais, protocolos seguros nativos dos serviços em nuvem e autenticação multifator, quando aplicável. A

AMARY CAPITAL

Amary Capital adota controles de acesso baseados em perfis, registro de atividades e monitoramento compatível com a criticidade dos sistemas.

No âmbito do PCN, a Amary Capital mantém estratégias estruturadas para assegurar a continuidade de suas operações críticas em situações de indisponibilidade, incidentes cibernéticos, falhas de terceiros, eventos de força maior, impossibilidade de acesso ao escritório ou indisponibilidade temporária de sistemas. Entre as principais medidas adotadas, destacam-se:

- utilização de infraestrutura em nuvem com recursos de disponibilidade, redundância e segregação compatíveis com a criticidade dos dados e sistemas;
- rotinas de backup automático ou periódico de dados críticos, com armazenamento seguro e testes regulares de restauração;
- procedimentos de recuperação de desastres, com tempos objetivos de recuperação e pontos objetivos de recuperação compatíveis com a criticidade dos processos;
- monitoramento dos ambientes tecnológicos e resposta estruturada a incidentes de segurança da informação;
- planos de contingência operacional que permitam a continuidade das atividades por meio de acesso remoto seguro, dispositivos autorizados e canais alternativos de comunicação;
- manutenção de contatos de emergência de prestadores críticos, administradores, custodiantes, corretoras, provedores de dados, tecnologia, nuvem e suporte;
- realização de testes periódicos do PCN e dos planos de recuperação, visando validar sua efetividade e promover melhorias contínuas.

Considerando o modelo operacional digital e flexível da Amary Capital, é permitido o trabalho remoto ou híbrido, desde que observadas as diretrizes de segurança da informação e continuidade. Colaboradores e Associados devem utilizar dispositivos autorizados e devidamente configurados, com controles como criptografia, proteção de endpoint, autenticação multifator, bloqueio de sessão, senha forte e acesso seguro aos sistemas corporativos.

A área de Tecnologia da Informação, interna ou terceirizada, é responsável pelo suporte aos Colaboradores e Associados, pela execução dos planos de resposta a incidentes e continuidade, e pela implementação de medidas corretivas ou preventivas. Sempre que necessário, poderão ser utilizadas ferramentas seguras de acesso remoto para suporte técnico, atualização de sistemas e correção de vulnerabilidades.

O uso dos sistemas, redes e informações da Amary Capital deve observar rigorosamente as políticas internas de segurança da informação e continuidade de negócios, sendo responsabilidade de cada

AMARY CAPITAL

Colaborador e Associado atuar de forma diligente na proteção dos ativos informacionais e na mitigação de riscos operacionais.

Colaboradores e Associados devem utilizar exclusivamente dispositivos, sistemas, meios tecnológicos e canais autorizados, abstendo-se do uso de dispositivos de armazenamento externos, contas pessoais, aplicativos não aprovados ou quaisquer outros recursos que não estejam diretamente relacionados ao desempenho de suas atividades profissionais ou que não tenham sido previamente aprovados pela área responsável.

Os ativos tecnológicos da Amary Capital, incluindo computadores, dispositivos móveis, sistemas corporativos, internet, e-mail, repositórios e demais ferramentas digitais, são disponibilizados prioritariamente para fins profissionais. O uso para finalidades pessoais deve ser eventual, moderado e não pode comprometer a produtividade, a segurança da informação, a disponibilidade dos sistemas ou o adequado funcionamento das atividades da Gestora.

É expressamente proibido o envio, compartilhamento ou armazenamento, por meio de sistemas e canais corporativos, de conteúdos discriminatórios, preconceituosos, obscenos, pornográficos, ofensivos, ilegais ou que violem princípios éticos e legais. Também é vedada a disseminação de mensagens, opiniões ou comentários que possam prejudicar a imagem, reputação ou integridade da Amary Capital, de seus Colaboradores, Associados, parceiros, fundos, investidores ou clientes.

O descumprimento destas diretrizes poderá sujeitar o Colaborador ou Associado às medidas disciplinares cabíveis, nos termos das políticas internas, contratos aplicáveis e legislação vigente.

5.1 Diretrizes para testes de continuidade de negócios

Para fins de simulação e planejamento, o PCN deve considerar, no mínimo, cenários de indisponibilidade crítica do edifício-sede, indisponibilidade de conectividade local, falha de provedor de nuvem, indisponibilidade de plataforma crítica de negociação ou risco, indisponibilidade de terceiro relevante, comprometimento de credenciais e incidente cibernético com potencial impacto operacional.

A resiliência operacional da Amary Capital fundamenta-se na utilização de infraestrutura em nuvem para armazenamento de documentos, bases de dados, relatórios, registros de auditoria e evidências, bem como na existência de canais alternativos de comunicação e acesso remoto seguro. Essa arquitetura busca reduzir a dependência da infraestrutura física local e permitir a continuidade de processos críticos em regime de contingência.

AMARY CAPITAL

Para o cenário de indisponibilidade crítica do escritório, estabelecem-se as seguintes métricas de recuperação, sujeitas a revisão conforme evolução da estrutura tecnológica e criticidade dos fundos sob gestão:

Processo	RTO	RPO	Observações
Gestão, trading e risco de fundos	Até 2 horas	Até 15 minutos	Prioridade máxima em horário de mercado.
Comunicação com administradores, custodiantes e corretoras	Até 2 horas	Até 30 minutos	Inclui contatos alternativos e canais corporativos.
Back office, middle office e conciliações	Até 4 horas	Até 4 horas	Priorização conforme liquidação e obrigações diárias.
Compliance, controles internos e evidências	Até 1 dia útil	Até 1 dia útil	Prazos regulatórios e contratuais prevalecem.
Documentos corporativos e repositórios	Até 4 horas	Até 30 minutos	Conforme disponibilidade do provedor de nuvem.

Os testes devem validar a eficácia da infraestrutura tecnológica e a capacidade da equipe em operar em regime de contingência, por trabalho remoto ou site alternativo. O escopo mínimo dos testes contempla:

- **Gestão e mesa de operações:** validar acesso remoto a sistemas de gestão de carteira, plataformas de negociação, dados de mercado, portais de corretoras e canais de comunicação com contrapartes, sem execução de ordens reais fora dos procedimentos aprovados.
- **Risco e controles de enquadramento:** validar acesso a relatórios de posições, limites, liquidez, exposição, alertas e evidências de aprovação ou escalonamento.
- **Back office e operacional:** executar simulação de batimento de carteira, conciliação, validação de arquivos e comunicação com administradores, custodiantes e demais prestadores.
- **Compliance e controles internos:** validar acesso a repositórios de políticas, registros, evidências, relatórios de incidentes, matriz de contatos e procedimentos de comunicação.
- **Tecnologia da Informação:** validar restauração de backup, suporte remoto, bloqueio e concessão de acessos, registro de eventos, resposta a incidente e comunicação com fornecedores críticos.

AMARY CAPITAL

Ao término de cada ciclo de teste, a área responsável deverá elaborar Relatório de Evidências de Continuidade, a ser submetido a Compliance, Diretoria ou Comitê aplicável. Os principais indicadores avaliados serão:

- eficácia de acesso remoto, incluindo autenticação, estabilidade, tempo de conexão e disponibilidade de sistemas críticos;
- adequação de infraestrutura, equipamentos, conexão e canais alternativos dos Colaboradores em regime de contingência;
- integridade e disponibilidade dos dados acessados durante o teste;
- efetividade dos backups e dos procedimentos de restauração;
- clareza dos papéis, responsáveis, escalonamentos e matriz de contatos;
- eventuais vulnerabilidades, incidentes, atrasos, falhas de autenticação, limitações de fornecedores ou necessidade de melhoria.

6. Política geral de proteção de dados

A Amary Capital adota diretrizes estruturadas para proteção de dados pessoais e continuidade de negócios, em conformidade com a LGPD, normas regulatórias aplicáveis e melhores práticas de mercado. Essas diretrizes são aplicáveis a todos os Colaboradores e Associados, abrangendo qualquer relação profissional, contratual, societária ou de confiança.

A operação da Amary Capital é predominantemente baseada em infraestrutura digital e serviços em nuvem. Nesse contexto, o tratamento de dados pessoais, incluindo coleta, armazenamento, uso, consulta, transmissão e compartilhamento, deve ocorrer em ambientes seguros, com controles de acesso, criptografia, monitoramento, registros e permissões adequadas, sempre respeitando os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

A Amary Capital poderá tratar dados pessoais de Colaboradores, Associados, sócios, representantes de prestadores, investidores, clientes, cotistas ou potenciais investidores, sempre que necessário ao cumprimento de obrigações legais, regulatórias, contratuais, legítimos interesses, exercício regular de direitos, prevenção a fraudes, execução de atividades de gestão de recursos ou outras bases legais aplicáveis.

A governança de proteção de dados é conduzida por Compliance, Controles Internos ou área designada pela Diretoria, responsável por supervisionar processos, manter políticas atualizadas, promover treinamentos, avaliar incidentes e assegurar a adoção de boas práticas em todas as áreas da

AMARY CAPITAL

organização. Todas as equipes possuem responsabilidade compartilhada na proteção das informações, devendo atuar de forma diligente na prevenção de riscos e no cumprimento das diretrizes internas.

No âmbito do PCN, a Amary Capital mantém medidas para garantir a continuidade de operações críticas em situações adversas, incluindo incidentes cibernéticos, indisponibilidade de sistemas ou eventos externos. Entre essas medidas destacam-se infraestrutura em nuvem com disponibilidade e redundância, backups seguros, procedimentos de recuperação, monitoramento, resposta estruturada a incidentes, acesso remoto seguro e testes periódicos de continuidade.

A Amary Capital mantém Plano de Resposta a Incidentes com procedimentos para identificação, contenção, análise, erradicação, recuperação e comunicação de eventos que possam comprometer a segurança das informações. Em caso de incidente relevante, serão avaliados impactos, dados afetados, titulares envolvidos, responsáveis, medidas corretivas e necessidade de comunicação a titulares, autoridades competentes, fundos, administradores fiduciários, prestadores e demais partes, conforme exigido pela regulamentação aplicável.

Por fim, a Amary Capital adota medidas técnicas e administrativas para proteger dados pessoais contra acessos não autorizados, perda, destruição, alteração, comunicação indevida ou qualquer forma de tratamento inadequado, incluindo ferramentas de segurança, controles de acesso, políticas internas, treinamento, registro de evidências e capacitação contínua de Colaboradores e Associados.

7. Terceiros críticos e computação em nuvem

A Amary Capital pode depender de terceiros críticos para a execução ou suporte de atividades essenciais, incluindo administradores fiduciários, custodiantes, corretoras, distribuidores, provedores de dados, plataformas de negociação, sistemas de risco, serviços de nuvem, e-mail corporativo, armazenamento de documentos, suporte de TI e segurança da informação.

A contratação, manutenção e substituição de terceiros críticos devem observar critérios compatíveis com a criticidade do serviço, o volume e sensibilidade dos dados acessados, o impacto potencial sobre fundos, investidores e atividades de gestão, a capacidade de continuidade do prestador, seus controles de segurança, acordos de nível de serviço, obrigações de confidencialidade e procedimentos de comunicação de incidentes.

Antes da contratação ou manutenção de terceiros críticos, a Amary Capital poderá realizar processo de diligência proporcional ao risco, incluindo avaliação de informações como:

- escopo do serviço, dados acessados, sistemas impactados e grau de dependência operacional;
- controles de segurança, autenticação, segregação, criptografia, logs, backups e retenção de dados;

AMARY CAPITAL

- planos de continuidade, recuperação de desastres, disponibilidade, redundância e histórico de incidentes;
- políticas de confidencialidade, proteção de dados, subcontratação, suporte, atendimento e escalonamento;
- localização, transferência, segregação e forma de armazenamento dos dados, quando aplicável;
- cláusulas contratuais sobre notificação de incidentes, auditoria, rescisão, portabilidade e eliminação ou devolução de dados.

Serviços de computação em nuvem utilizados pela Amary Capital devem ser avaliados considerando segurança, disponibilidade, capacidade de recuperação, controle de acessos, segregação lógica, criptografia, trilhas de auditoria, subcontratados relevantes, localização e possibilidade de migração ou substituição. A Amary Capital deve manter plano de saída ou medida alternativa razoável para serviços cuja indisponibilidade possa comprometer operações críticas.

Incidentes, falhas relevantes ou alterações materiais envolvendo terceiros críticos devem ser avaliados pelas áreas responsáveis e, quando necessário, escalados à Diretoria, Compliance, Risco, Tecnologia da Informação, Comitê aplicável, administradores fiduciários, fundos ou autoridades competentes.

8. Vigência e atualização

O presente Manual entra em vigor na data de sua aprovação pela instância competente da Amary Capital e deve ser revisado, no mínimo, anualmente, ou em periodicidade inferior sempre que houver necessidade de atualização em decorrência de alterações regulatórias, mudanças nos processos internos, alterações relevantes em sistemas, substituição de terceiros críticos, evolução tecnológica, testes de continuidade, incidentes, auditorias ou identificação de novos riscos.

A Amary Capital poderá promover revisões extraordinárias a qualquer tempo, com o objetivo de assegurar aderência às melhores práticas de mercado, à legislação aplicável, às normas de autorregulação e à efetividade dos controles de segurança da informação, proteção de dados e continuidade de negócios.

Eventuais alterações serão devidamente comunicadas aos Colaboradores e Associados, que deverão manter-se atualizados e em conformidade com as diretrizes vigentes. O histórico de versões, aprovações e evidências de comunicação deverá ser mantido em repositório apropriado.

Anexo I. Matriz de acionamento do PCN

A matriz abaixo apresenta critérios mínimos para acionamento do PCN. A avaliação concreta deve considerar horário de mercado, fundos afetados, sistemas impactados, riscos aos investidores, prazos regulatórios, dependência de terceiros e possibilidade de continuidade por meios alternativos.

Cenário	Gatilho	Responsável inicial	Ação imediata
Indisponibilidade do escritório	Acesso físico ao escritório indisponível por prazo superior a 30 minutos em dia útil.	Diretoria / TI	Acionar trabalho remoto seguro e testar acesso a sistemas críticos.
Indisponibilidade de internet local	Falha de conectividade que prejudique gestão, trading, risco ou comunicações críticas.	TI / Gestores	Usar conexão alternativa, trabalho remoto ou site alternativo.
Falha em plataforma de negociação ou risco	Incapacidade de acessar sistema crítico durante horário de mercado.	Gestão / Risco	Acionar fornecedor, usar canal alternativo e comunicar responsáveis.
Incidente cibernético	Suspeita de comprometimento de credenciais, malware, vazamento ou acesso não autorizado.	TI / Compliance	Conter, preservar evidências, bloquear acessos e avaliar comunicações.
Falha de terceiro crítico	Administrador, custodiante, corretora, provedor de nuvem ou dados indisponível ou com incidente relevante.	Operacional / Compliance	Acionar contatos de contingência e avaliar impacto nos fundos.

Anexo II. Registro mínimo de incidentes

Todo incidente operacional, tecnológico, cibernético ou de proteção de dados deve ser registrado em repositório apropriado, com nível de detalhe compatível com sua materialidade. O registro mínimo deve contemplar:

- data e horário de identificação e encerramento do incidente;

- área ou pessoa que identificou o incidente;
- sistemas, dados, fundos, prestadores ou processos afetados;
- descrição do evento, causa provável e evidências disponíveis;
- classificação de severidade, impacto operacional, impacto regulatório e impacto sobre dados pessoais;
- medidas de contenção, correção, recuperação e prevenção adotadas;
- responsáveis internos e externos envolvidos;
- necessidade de comunicação a Diretoria, Comitê, administrador fiduciário, clientes, titulares de dados, CVM, ANBIMA, ANPD ou outros órgãos;
- lições aprendidas, planos de ação e prazos de implementação.

Os registros de incidentes e relatórios pós-incidente devem ser mantidos pelo prazo definido em política interna ou pelo prazo legal e regulatório aplicável, o que for maior, observando regras de confidencialidade e proteção de dados.