POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

CAPRI INVESTIMENTOS LTDA.

("Sociedade")

AGOSTO/2026

CAPÍTULO I
DO OBJETIVO

1.1. O presente instrumento tem por objetivo estabelecer regras, princípios, procedimentos e controles para a segurança da informação e a segurança cibernética da Sociedade, visando preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a rastreabilidade das informações e dos ativos utilizados em suas atividades de gestão profissional de recursos de terceiros.

1.2. Esta Política aplica-se aos sócios, diretores, funcionários, estagiários e demais colaboradores da Sociedade, bem como, no que couber, aos terceiros e prestadores de serviços relevantes que tenham acesso a informações, dados, sistemas, infraestrutura ou ativos da Sociedade, de seus fundos sob gestão, investidores ou clientes ("Colaboradores"). Os Colaboradores devem atestar ciência e adesão às regras aplicáveis e participar dos treinamentos previstos nesta Política.

1.3. A Sociedade exigirá compromisso de confidencialidade dos terceiros relevantes que tenham acesso a informações confidenciais ou privilegiadas, salvo quando obrigação equivalente já estiver prevista no respectivo contrato de prestação de serviços.

1.4. Esta Política será revisada, no mínimo, anualmente e sempre que houver alteração relevante na regulação ou autorregulação aplicável, na estrutura tecnológica, no modelo de negócio, no perfil de risco ou nos controles da Sociedade, sendo mantido controle de versões e promovida a comunicação das alterações aos Colaboradores.

1.5. Em caso de dúvidas, suspeita de incidente, necessidade de aconselhamento ou exceção a esta Política, o Colaborador deve buscar orientação prévia junto ao Diretor de Compliance da Sociedade.

1.6. Para fins desta Política, consideram-se "Ativos de Informação" os dados, documentos, sistemas, aplicações, credenciais, equipamentos, redes, processos, ambientes em nuvem e demais recursos que suportem as atividades da Sociedade. Consideram-se "Informações Confidenciais ou Privilegiadas" aquelas não públicas cuja divulgação, alteração, perda ou uso indevido possa afetar a Sociedade, seus fundos, investidores, clientes, contrapartes ou terceiros, inclusive dados pessoais, informações de investimento e informações sujeitas a barreiras de informação.

1.7. As informações serão tratadas de acordo com sua sensibilidade e necessidade de acesso, observando-se, no mínimo, as categorias Pública, Interna e Confidencial/Privilegiada. O acesso deverá observar os princípios de necessidade de conhecimento ("need to know"), menor privilégio ("least privilege") e segregação de funções.

1.8. O Diretor de Compliance é responsável pela coordenação e supervisão desta Política, sem prejuízo das atribuições da Diretoria e do suporte da área interna ou do prestador de serviços de Tecnologia da Informação ("TI"). Todos os Colaboradores são responsáveis pelo cumprimento das regras que lhes sejam aplicáveis e pela comunicação tempestiva de incidentes ou vulnerabilidades identificadas.

CAPÍTULO II
PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

I. Acesso Restrito

2.1.1. A troca de informações deve observar a necessidade efetiva de acesso para o desempenho das atividades do receptor, as barreiras de informação aplicáveis e a classificação da informação. Em caso de dúvida, a área de Compliance deve ser consultada previamente à revelação ou ao compartilhamento.

2.1.2. Os Colaboradores com acesso a sistemas, dados ou ativos da Sociedade devem adotar as precauções necessárias para impedir acessos não autorizados, preservando credenciais, tokens, chaves, dispositivos de autenticação e demais meios de acesso, sendo vedado o seu compartilhamento.

2.1.3. O acesso a pastas, arquivos, sistemas e aplicações será individualizado, autenticado e concedido conforme o perfil funcional do usuário, de modo a permitir a identificação e a rastreabilidade dos acessos e impedir a utilização por pessoas não autorizadas.

2.1.4. As comunicações realizadas por meio dos recursos corporativos da Sociedade devem permitir, quando tecnicamente aplicável, a identificação de remetente, destinatário e usuário responsável, observados os controles de registro e monitoramento definidos pela Sociedade.

2.1.5. O armazenamento de Informações Confidenciais ou Privilegiadas em dispositivos portáteis deve restringir-se a equipamentos fornecidos, administrados ou expressamente homologados pela Sociedade, com os controles de segurança aplicáveis.

2.1.6. A concessão, alteração e revogação de acessos será coordenada pelo Diretor de Compliance, com apoio de TI, observando-se a segregação de funções, o princípio de menor privilégio e o ciclo de vida do acesso desde a admissão, mudança de função ou área, afastamento relevante e desligamento.

2.1.7. As credenciais de acesso devem observar requisitos mínimos de complexidade e segurança definidos pela Sociedade e/ou pelos sistemas utilizados. Sempre que tecnicamente disponível e proporcional ao risco, será exigida autenticação multifator ("MFA"), especialmente para e-mail corporativo, serviços em nuvem, acessos remotos e sistemas críticos. Tentativas malsucedidas e eventos relevantes de autenticação deverão ser registrados e tratados pelos controles de TI.

2.1.8. Após período máximo de inatividade definido pela Sociedade, os dispositivos e sistemas deverão bloquear a sessão e exigir nova autenticação do usuário para retomada do acesso.

2.1.9. No desligamento de Colaborador, os acessos internos devem ser bloqueados e as credenciais revogadas tempestivamente. Para sistemas externos, a Sociedade deverá solicitar a revogação imediatamente e acompanhar sua efetiva conclusão. A mesma lógica deverá ser aplicada, conforme o risco, a mudanças de função e afastamentos.

2.1.10. O acesso a informações confidenciais em meio físico ou eletrônico deverá observar segregação física, lógica e funcional, conforme aplicável às atividades da Sociedade e às barreiras de informação existentes.

2.1.11. O acesso remoto deverá ocorrer por meios seguros e homologados pela Sociedade, preferencialmente em equipamentos corporativos ou administrados, com criptografia de comunicação e mecanismos de autenticação apropriados. O uso de redes públicas ou não confiáveis para acesso a Informações Confidenciais ou Privilegiadas deve ser evitado ou protegido por solução segura aprovada pela Sociedade.

2.1.12. A Sociedade realizará revisão periódica de acessos e privilégios, no mínimo semestralmente para os sistemas e ambientes críticos, de modo a verificar a adequação dos perfis concedidos e promover a correção tempestiva de acessos desnecessários ou incompatíveis.

II. Backup

2.2.1. Os documentos e dados relevantes mantidos nos ambientes corporativos da Sociedade serão objeto de backup periódico, com frequência compatível com a criticidade das informações e, para os principais repositórios de trabalho, no mínimo diária, preferencialmente com versionamento e registro das alterações.

2.2.2. Os backups deverão ser protegidos contra acesso não autorizado e contra comprometimento simultâneo com o ambiente de produção, observando-se, quando tecnicamente disponível, controles de segregação, criptografia, retenção e proteção contra alteração indevida.

2.2.3. A capacidade de recuperação deverá ser validada por testes de restauração periódicos, com evidências dos testes e tratamento das falhas identificadas, em alinhamento com o Plano de Continuidade de Negócios.

III. Cópia de Arquivos e instalações

2.3.1. Programas, aplicações, extensões, serviços e ferramentas utilizados pelos Colaboradores nos equipamentos ou ambientes corporativos devem ser previamente homologados pela área responsável por TI e/ou pelo Compliance. Downloads e instalações deverão possuir justificativa compatível com as atividades profissionais e respeitar os controles de segurança aplicáveis.

2.3.2. A cópia de arquivos e a instalação de programas devem respeitar os direitos de propriedade intelectual, licenças, patentes e demais requisitos legais e contratuais aplicáveis.

2.3.3. É vedado copiar, transferir, encaminhar ou circular externamente arquivos da Sociedade fora dos meios e finalidades profissionais autorizados. Quando o compartilhamento externo for necessário para execução das atividades, o Colaborador deverá adotar meio aprovado, limitar o conteúdo ao estritamente necessário e preservar a integridade e a confidencialidade da informação.

2.3.4. Documentos impressos que contenham informações restritas ou confidenciais deverão ser retirados imediatamente da impressora, mantidos sob guarda adequada e descartados de forma segura, sendo vedada sua permanência desnecessária em mesas, impressoras, copiadoras ou áreas de circulação.

2.3.5. É vedado inserir Informações Confidenciais ou Privilegiadas, dados pessoais não públicos, credenciais, documentos internos ou arquivos da Sociedade em ferramentas de inteligência artificial, plataformas públicas, extensões de navegador ou outros serviços digitais não homologados. O uso de ferramentas de inteligência artificial ou automação deverá restringir-se às soluções aprovadas pela Sociedade e observar os mesmos controles de acesso, confidencialidade, finalidade e retenção aplicáveis às demais ferramentas corporativas.

IV. Descarte de Informações

2.4.1. O descarte de informações confidenciais ou de mídias que as contenham deverá observar procedimentos que impeçam sua recuperação indevida, incluindo, conforme aplicável:

(i) exclusão segura do conteúdo ou destruição da mídia, de modo a impedir acesso não autorizado;

(ii) trituração ou descarte seguro de documentos físicos que contenham informações protegidas;

(iii) documentação do descarte final quando realizado por terceiro relevante; e

(iv) apagamento seguro ou destruição de dispositivos de memória e armazenamento desativados, incluindo notebooks, dispositivos USB, discos rígidos, tablets e smartphones, de modo a tornar irrecuperáveis as informações protegidas neles existentes.

V. Redundância

2.5.1. Além das cópias de segurança, a Sociedade deverá manter recursos de TI e alternativas de acesso compatíveis com a criticidade de seus processos. Em caso de indisponibilidade física do local de trabalho, a equipe-chave previamente designada poderá acessar, por meio seguro, os ambientes e informações necessários à continuidade das atividades.

2.5.2. A Sociedade deverá manter medidas de contingência para falhas de energia, conectividade, equipamentos ou serviços relevantes, observando o Plano de Continuidade de Negócios e os recursos efetivamente disponíveis, incluindo soluções de energia de contingência, redundância de conectividade ou ambientes alternativos, conforme aplicável.

VI. Serviços de Processamento, Armazenamento e Computação em Nuvem

2.6.1. A contratação de serviços de processamento, armazenamento de dados e computação em nuvem, no Brasil ou no exterior, classificados pela Sociedade como críticos ou de maior risco, deverá ser precedida de avaliação compatível com a criticidade do serviço e com os riscos envolvidos.

2.6.2. A diligência do prestador deverá considerar, no mínimo, a capacidade de acesso da Sociedade aos dados, a confidencialidade, a integridade, a disponibilidade e a recuperação das informações, certificações relevantes quando aplicáveis, mecanismos de monitoramento, segregação de dados, controles de identidade e acesso, continuidade do serviço, subcontratações relevantes e obrigações de comunicação de incidentes.

2.6.3. Os contratos com prestadores relevantes deverão conter, quando aplicável, obrigações de confidencialidade, segurança, disponibilidade, cooperação em incidentes, devolução ou eliminação de dados e acesso às informações necessárias à supervisão do serviço.

2.6.4. A Sociedade deverá monitorar os prestadores críticos ou de maior risco ao longo da relação contratual e poderá utilizar, como referência, questionários de due diligence disponibilizados pela ANBIMA e outras evidências compatíveis com o risco do serviço.

VII. Dados Pessoais e Ciclo de Vida da Informação

2.7.1. O tratamento de dados pessoais deverá observar a legislação aplicável e as políticas internas de privacidade da Sociedade. Os controles de segurança deverão contemplar a proteção da informação ao longo de seu ciclo de vida, incluindo geração, recebimento, armazenamento, acesso, uso, compartilhamento, transmissão, transporte, retenção e descarte.

CAPÍTULO III
SUPORTE E MONITORAMENTO

3.1. Falhas de rede, equipamento, sistema, aplicação ou serviço relevante deverão ser comunicadas tempestivamente ao Diretor de Compliance e/ou ao responsável por TI, que providenciarão o suporte interno ou externo necessário e avaliarão eventual acionamento de contingência.

3.2. Os sistemas, dispositivos, redes e demais recursos corporativos poderão ser revisados e monitorados pela Sociedade, observada a legislação aplicável, com o objetivo de detectar acessos indevidos, irregularidades, vazamentos, malware, transferências não autorizadas e outros eventos de segurança.

3.3. Os recursos de comunicação corporativa, incluindo e-mail e demais canais homologados, destinam-se prioritariamente a fins profissionais e poderão ser monitorados pela Sociedade nos limites da legislação e das políticas internas aplicáveis.

3.4. Qualquer suspeita ou conhecimento de violação desta Política, vazamento de informação, perda de dispositivo, comprometimento de credencial, mensagem de phishing, malware ou outro incidente de segurança deverá ser comunicado imediatamente ao Compliance e/ou TI para apuração, contenção, mitigação, correção e, quando cabível, responsabilização.

3.5. Poderão ser realizadas inspeções periódicas, inclusive sem aviso prévio, nos equipamentos e ambientes corporativos para verificar softwares, configurações, downloads, acessos e arquivos incompatíveis com esta Política.

Tratamento de casos de vazamento de informações confidenciais

3.6. Em caso de vazamento ou suspeita de vazamento de Informações Confidenciais ou Privilegiadas, inclusive dados pessoais, o Diretor de Compliance deverá coordenar, com apoio de TI e das demais áreas relevantes, a avaliação do evento e da necessidade de comunicação aos investidores, clientes, titulares, prestadores, autoridades ou demais partes afetadas, observados os requisitos e prazos legais, regulatórios e contratuais aplicáveis.

3.7. A Sociedade acionará o seu Plano de Resposta a Incidentes e, quando necessário, o Plano de Continuidade de Negócios, buscando identificar a causa, conter o evento, preservar evidências, recuperar os serviços afetados e implementar medidas corretivas. Deverá ser elaborado relatório do incidente com, quando aplicável, escopo, sistemas e informações afetados, impactos operacionais, financeiros, legais e reputacionais, medidas adotadas e plano de remediação.

3.8. O relatório do incidente será coordenado pelo Diretor de Compliance e submetido à Diretoria quando a materialidade ou a severidade assim exigirem, sendo acompanhada a implementação das medidas corretivas até sua conclusão.

Firewall

3.9. A Sociedade deverá manter controles técnicos proporcionais aos riscos identificados, incluindo firewall e filtragem de tráfego, proteção antimalware e/ou de endpoint, proteção de e-mail, bloqueio de conteúdos ou conexões maliciosas, atualizações de segurança, autenticação adequada e demais mecanismos compatíveis com a infraestrutura utilizada.

Testes de Segurança

3.10. As seguintes rotinas mínimas devem ser observadas para monitoramento dos sistemas e controles utilizados, podendo ser ajustadas conforme a arquitetura tecnológica, o risco e os serviços contratados:

ROTINAS OPERACIONAIS	PERIODICIDADE
Proteção antimalware/endpoint e varredura de ameaças	Tempo real ou conforme tecnologia utilizada
Controle de conteúdo e tráfego por firewall e ferramentas de segurança	Tempo real
Monitoramento de autenticação e tentativas malsucedidas	Tempo real ou conforme capacidade do sistema
Bloqueio automático de tela por inatividade	No máximo a cada 15 min
Backup dos principais repositórios de trabalho	Diário
Backup de configurações críticas de segurança	A cada alteração relevante
Verificação do status e logs de backup	Diário
Teste de restauração de backup	Mensal
Atualizações de sistema operacional e correções de segurança	Semanal ou tempestivamente para correções críticas
Verificação da proteção dos endpoints	Semanal
Reinicialização/manutenção programada de estações, quando necessária	Semanal ou conforme necessidade técnica
Revisão de acessos e privilégios de ambientes críticos	Semestral
Verificação da autenticação multifator nos ambientes em que for exigida	Contínua e nas revisões de acesso

CAPÍTULO IV
IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS CIBERNÉTICOS

4.1. A Sociedade deverá identificar os Ativos de Informação relevantes para o desempenho de suas atividades, incluindo, conforme aplicável: (i) sistemas de boletagem, negociação, gestão, risco e conciliação; (ii) aplicações e provedores de dados e de mercado; (iii) e-mail e ferramentas de colaboração; (iv) serviços em nuvem; (v) redes, equipamentos e dispositivos; (vi) credenciais e mecanismos de autenticação; (vii) dados e documentos de fundos, investidores e clientes; e (viii) processos operacionais críticos.

4.2. A avaliação de riscos deverá considerar ameaças internas e externas, incluindo malware e ransomware, engenharia social, phishing, vishing e smishing, furto ou comprometimento de credenciais, acesso não autorizado, falhas ou configurações inadequadas, ataques de negação de serviço, ameaças persistentes, perda ou furto de equipamentos, vulnerabilidades de terceiros e da cadeia de fornecimento, indisponibilidade de serviços em nuvem e vazamento de dados.

4.3. Para cada risco relevante, a Sociedade deverá avaliar os ativos afetados, vulnerabilidades internas e externas, probabilidade de ocorrência, magnitude dos impactos potenciais, controles existentes, risco residual, responsáveis e, quando necessário, plano de ação para tratamento do risco.

4.4. A avaliação de riscos cibernéticos deverá ser revisada no mínimo anualmente e sempre que houver mudança tecnológica relevante, contratação ou substituição de prestador crítico, implantação de novo sistema relevante, alteração significativa de processo ou ocorrência de incidente material.

4.5. Os inventários de hardware, software, aplicações, serviços em nuvem e demais Ativos de Informação relevantes deverão ser mantidos atualizados em nível compatível com o porte e a complexidade da Sociedade.

CAPÍTULO V
AÇÕES DE PROTEÇÃO E PREVENÇÃO AOS RISCOS CIBERNÉTICOS

5.1. Os planos de prevenção e proteção descritos neste Capítulo têm por objetivo reduzir a probabilidade e o impacto de incidentes cibernéticos, de acordo com os riscos identificados e com a criticidade dos Ativos de Informação.

5.2. A Sociedade adotará controles de acesso físico e lógico compatíveis com seu porte, perfil de risco, modelo de negócio e complexidade, destinados a identificar, autenticar e autorizar usuários e impedir acessos não autorizados a sistemas, dados e ativos.

5.3. Os Colaboradores devem observar as regras de credenciais, autenticação, segregação de funções, uso de equipamentos, compartilhamento de informações e barreiras de informação previstas nesta Política e nas demais normas internas da Sociedade.

5.4. Eventos relevantes de login, autenticação, alteração de credenciais e acesso a sistemas críticos deverão ser rastreáveis e auditáveis na medida da capacidade técnica dos sistemas. Inconsistências, acessos incompatíveis ou indícios de comprometimento deverão ser reportados e tratados tempestivamente.

5.5. Sem prejuízo de outros riscos identificados, a Sociedade observará as seguintes ações mínimas de proteção e prevenção:

Risco	Ação de Proteção/Prevenção
Tentativa de invasão ou acesso não autorizado	Uso de firewall, controles de acesso, registro de eventos, bloqueios automáticos quando disponíveis, revisão de privilégios e monitoramento de alertas.
Phishing, engenharia social e furto de credenciais	Treinamento e conscientização, filtros de e-mail, MFA nos ambientes aplicáveis, validação de solicitações sensíveis e comunicação imediata de mensagens suspeitas.
Malware e ransomware	Proteção antimalware/endpoint, atualizações de segurança, restrição de software, backups segregados, testes de restauração e resposta coordenada a incidentes.
Vazamento ou transferência indevida de informações	Classificação da informação, necessidade de conhecimento, meios corporativos homologados, criptografia quando aplicável, restrição a ferramentas não autorizadas e monitoramento compatível com o risco.
Indisponibilidade de sistema, rede ou provedor	Redundância e contingência compatíveis com a criticidade, backups, alternativas de acesso e acionamento do Plano de Continuidade de Negócios.
Risco de terceiros e serviços em nuvem	Diligência prévia, requisitos contratuais, controles de acesso e segregação, monitoramento do prestador, gestão de incidentes e plano de substituição/continuidade quando aplicável.

5.6. Novos equipamentos, sistemas e aplicações relevantes devem ser submetidos a configuração segura, homologação e testes compatíveis com o risco antes de sua entrada em produção. Alterações relevantes na infraestrutura devem ser avaliadas quanto a vulnerabilidades e impactos de segurança.

5.7. Programas, aplicações e extensões não autorizados são vedados nos ambientes corporativos. Instalações, downloads e alterações de configuração deverão observar os procedimentos definidos por TI e/ou Compliance.

5.8. A Sociedade deverá utilizar criptografia ou mecanismos de proteção equivalentes para transmissão de Informações Confidenciais ou Privilegiadas e, quando tecnicamente aplicável e proporcional ao risco, para seu armazenamento.

5.9. Vulnerabilidades e atualizações de segurança deverão ser acompanhadas pela Sociedade ou pelo prestador de TI, com priorização de correções críticas e de exposições relevantes. Falhas identificadas em testes ou monitoramentos deverão gerar registro e plano de tratamento compatível com a severidade.

5.10. A autenticação multifator deverá ser utilizada nos ambientes definidos como críticos ou de maior risco sempre que tecnicamente disponível, especialmente em serviços de e-mail, nuvem, acesso remoto e sistemas administrativos relevantes.

CAPÍTULO VI
MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA

6.1. A Sociedade realizará rotinas de verificação, monitoramento e testes para identificar anomalias, ameaças, vulnerabilidades, acessos indevidos, componentes ou dispositivos não autorizados e falhas de efetividade dos controles:

Rotina	Periodicidade mínima
Verificação de execução dos backups críticos	Diário
Teste de restauração de dados	Mensal
Teste de invasão externa e/ou avaliação técnica equivalente, conforme escopo definido por risco	Semestral
Simulação de phishing ou exercício equivalente de conscientização	Semestral
Teste de resposta a incidentes com simulação de cenários	Semestral
Análise de logs e trilhas de auditoria de sistemas críticos	Diário ou conforme capacidade do sistema e criticidade
Revisão de acessos e privilégios críticos	Semestral
Análise de vulnerabilidade da infraestrutura relevante	No mínimo anual e após alteração tecnológica relevante
Validação geral da efetividade do programa de segurança da informação e cibernética	No mínimo anual

6.2. Serão mantidos inventários atualizados de hardware, software, aplicações e serviços relevantes. Periodicamente, e no mínimo semestralmente para os itens críticos, serão realizadas verificações destinadas a identificar equipamentos, aplicações ou acessos não autorizados e softwares sem licenciamento ou homologação adequados.

6.3. Sempre que houver alteração relevante na estrutura tecnológica, nos sistemas críticos ou na contratação de prestador crítico, será avaliada a necessidade de análise de vulnerabilidade, teste específico ou revisão do risco.

6.4. O acompanhamento dos controles deverá utilizar, quando aplicável, métricas, critérios, indicadores, registros de falhas, alertas, incidentes, vulnerabilidades e planos de ação, permitindo verificar a efetividade dos controles e identificar deficiências.

6.5. Os testes e validações deverão ser documentados em nível compatível com sua relevância. Deficiências materiais ou recorrentes serão reportadas ao Diretor de Compliance e, conforme a gravidade, à Diretoria, com definição de responsável, prazo e acompanhamento da remediação.

CAPÍTULO VII
RESPOSTAS A INCIDENTES CIBERNÉTICOS

7.1. Todo incidente ou suspeita de incidente deverá ser comunicado imediatamente ao Compliance e/ou TI e classificado de acordo com sua severidade, considerando o impacto sobre confidencialidade, integridade e disponibilidade das informações, continuidade das atividades, dados pessoais, investidores, clientes e obrigações legais ou regulatórias:

Severidade	Critério indicativo	Tratamento e escalonamento
Leve	Evento localizado, sem impacto material identificado e com contenção simples.	Tratamento operacional, registro quando aplicável e comunicação ao Compliance.
Média	Impacto limitado ou potencial sobre sistema, informação ou processo relevante, exigindo investigação e medidas de contenção.	Atuação coordenada de Compliance e TI, preservação de evidências e acompanhamento até a normalização.
Grave	Comprometimento material, indisponibilidade relevante, vazamento de informação sensível, impacto a investidores/clientes ou potencial obrigação de comunicação externa.	Acionamento imediato do Diretor de Compliance, TI, Diretoria e demais áreas necessárias; avaliação de continuidade, comunicação externa e contratação de especialistas, se cabível.

7.2. Compete ao Compliance coordenar a comunicação interna da contingência e orientar os Colaboradores sobre a postura e as providências cabíveis, em conjunto com TI e demais áreas envolvidas e em observância ao Plano de Continuidade de Negócios.

7.3. O tratamento de incidentes deverá considerar, conforme aplicável, as etapas de identificação e triagem, contenção, preservação de evidências, erradicação da causa, recuperação dos ambientes e serviços, validação do retorno à normalidade e acompanhamento das medidas corretivas.

7.4. O Compliance coordenará relatório do incidente contendo, na medida do possível, natureza e causa, ativos e informações afetados, período de exposição, impactos operacionais, financeiros, legais e reputacionais, medidas de contenção e recuperação, comunicações realizadas, responsáveis e plano de remediação. Incidentes relevantes serão submetidos à Diretoria.

7.5. A Sociedade deverá avaliar, conforme a natureza do incidente, a necessidade e o prazo de comunicação a investidores, clientes, titulares de dados, prestadores de serviços, CVM, ANBIMA, ANPD, autoridades policiais ou outras autoridades competentes, quando exigido pela legislação, regulação, autorregulação ou contratos aplicáveis.

7.6. Logs, registros, evidências, imagens, mensagens, arquivos e demais elementos relevantes ao incidente deverão ser preservados de forma compatível com a investigação, eventual perícia e obrigações de manutenção de registros.

7.7. Após o retorno à normalidade, deverá ser realizada análise de causa e de lições aprendidas, com definição das melhorias necessárias para reduzir a probabilidade ou o impacto de recorrência. As medidas relevantes deverão ser incorporadas aos controles, à avaliação de riscos, ao Plano de Continuidade de Negócios e/ou a esta Política, conforme aplicável.

7.8. Os prestadores de serviços críticos ou de maior risco deverão estar sujeitos, na medida aplicável, a obrigações de comunicação e cooperação em incidentes que possam afetar os dados, sistemas ou atividades da Sociedade.

CAPÍTULO VIII
PROGRAMA DE TREINAMENTO

8.1. A Sociedade manterá programa de treinamento e conscientização aplicável aos Colaboradores e, no que couber, a terceiros relevantes, abrangendo proteção de dados, segurança da informação, segurança cibernética, confidencialidade, prevenção de incidentes e protocolos de continuidade.

8.2. Os procedimentos e rotinas desta Política serão abordados no treinamento de integração dos novos Colaboradores e em treinamento periódico, no mínimo anual, coordenado pelo Diretor de Compliance ou por terceiro contratado para essa finalidade.

8.3. Poderão ser realizados treinamentos extraordinários sempre que houver mudanças relevantes de risco, tecnologia, procedimentos, incidentes, ameaças ou regulação, bem como para grupos expostos a riscos específicos.

8.4. O programa poderá incluir simulações de phishing, exercícios de resposta a incidentes, comunicações de conscientização e testes de conhecimento. A Sociedade deverá manter evidências dos treinamentos e das principais ações de conscientização realizadas.

CAPÍTULO IX
DISPOSIÇÕES GERAIS E ENFORCEMENT

9.1. Os documentos, relatórios, evidências de testes, registros de treinamento, avaliações, planos de ação e informações relevantes aos procedimentos e controles descritos nesta Política serão mantidos em meio físico ou eletrônico pelo prazo mínimo de 5 (cinco) anos, sem prejuízo de prazos superiores exigidos por lei, regulação, autorregulação, contrato ou necessidade de investigação.

9.2. O presente instrumento prevalece sobre entendimentos orais ou escritos anteriores sobre as matérias nele tratadas, sem prejuízo das demais políticas, manuais e procedimentos internos da Sociedade, que devem ser interpretados de forma complementar.

9.3. O descumprimento desta Política poderá resultar em medidas disciplinares proporcionais à gravidade, à recorrência e às circunstâncias da violação, incluindo advertência, suspensão, desligamento, rescisão contratual e demais medidas cabíveis, sem prejuízo de eventual responsabilização civil, administrativa ou criminal.

9.4. Esta Política será revisada, no mínimo, anualmente e sempre que houver alteração relevante na regulação ou autorregulação aplicável, na estrutura tecnológica, no perfil de risco, no modelo de negócio ou nos controles da Sociedade.

9.5. A versão vigente desta Política será mantida sob controle documental e disponibilizada aos Colaboradores e, quando aplicável, à CVM, ANBIMA ou demais autoridades competentes, observados os canais e prazos previstos na regulação e autorregulação vigentes.

9.6. As alterações desta Política serão submetidas à aprovação da instância competente da Sociedade e produzirão efeitos a partir da data de sua aprovação, devendo a versão aprovada substituir a versão anterior nos repositórios oficiais.

Controle de versões

Versão	Status/ Responsável	Descrição
Dezembro/2023	Vencida / Leonardo Moreira	Versão utilizada como documento-base para esta atualização.
Agosto/2026	Vigente / Diego Salvatti	Atualização regulatória e de melhores práticas de segurança da informação e segurança cibernética.

Referências normativas principais: Resolução CVM nº 21/2021, em sua versão consolidada; Código ANBIMA de Administração e Gestão de Recursos de Terceiros; Regras e Procedimentos ANBIMA de Deveres Básicos; Lei nº 13.709/2018 (LGPD), quando aplicável; e Guia de Cibersegurança da ANBIMA como referência de boas práticas.