ATMOSPHERE CAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

FEVEREIRO

2026

Sumário

1. INTRODUÇÃO E OBJETIVOS

A ATMOSPHERE reconhece que informação, tecnologia e processos de negócio são ativos estratégicos. A proteção desses ativos é essencial para assegurar a continuidade dos serviços, a confiança de clientes e contrapartes e o atendimento às exigências legais e regulatórias aplicáveis ao mercado financeiro.

Esta Política estabelece princípios, responsabilidades e controles para garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações, bem como promover a resiliência operacional diante de incidentes cibernéticos e situações de contingência.

2. ABRANGÊNCIA

Aplica-se a colaboradores, diretores, estagiários, prestadores de serviço, fornecedores e terceiros que, de forma direta ou indireta, tenham acesso às informações, sistemas, instalações físicas ou ativos tecnológicos da ATMOSPHERE, em ambientes internos, remotos e em nuvem.

3. GOVERNANÇA E RESPONSABILIDADES

3.1. Segurança da Informação e Cibersegurança

Caberá à Suporte de Tecnologia (TI) e ao Compliance, elaborar e manter atualizado risk assessement com o objetivo de identificar e avaliar eventuais riscos em que os processos e ativos relevantes da ATMOSPHERE estejam sujeitos em virtude das vulnerabilidades e possíveis cenários de ameaça atribuídos a cada processo ou ativo. Na avaliação dos riscos identificados, deverão ser considerados possíveis impactos financeiros, operacionais e reputacionais, assim como a expectativa de concretização dos riscos. Uma vez identificados os riscos, ações de prevenção e proteção devem ser tomadas pelo TI e pelo Compliance.

A ATMOSPHERE possui uma infraestrutura adequada com Switchs, roteador wi-fi, Gateway de Internet (responsável pela redundância de internet) , firewall , no-breaks, interligando as unidades de equipamentos, computadores, além de aparelhos de telefônicos;

Os sistemas de computadores, telecomunicação e mídia da ATMOSPHERE passam por testes periódicos e monitoramentos sem aviso prévio ou permissão. Os testes periódicos serão realizados pela área Suporte de Tecnologia (TI) sob a coordenação da área de Compliance. Tais testes consistem no mínimo (i) em revisões e monitoramentos dos sistemas de informações, criando simulações de violações interna e externa de acessos, permissões e autorizações; e (ii) em verificações da possiblidade de falhas de segurança que possibilitem uso ou acesso não autorizados de servidores e equipamentos eletrônicos.

Os testes periódicos acima mencionados visam assegurar (i) o controle e restrição adequados dos acessos lógicos e seus respectivos privilégios dos usuários; (ii) as medidas necessárias para que nenhum usuário possua credenciais de acesso com privilégios além dos mínimos necessários para o desempenho de suas funções; (iii) a tempestiva procedência de ações necessárias e suficientes para impedir o acesso de usuários quando necessário; (iv) a execução de ações para implementar as diretrizes previstas na política de segurança; (v) a utilização dos sistemas de informação exclusivamente para as atividades corporativas; (vi) o uso correto e permitido de informações confidenciais por colaboradores; e (vii) o estrito cumprimento pelos colaboradores das políticas internas da ATMOSPHERE.

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A ATMOSPHERE adota como princípios: confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade, que orientam os controles técnicos, administrativos e físicos aplicáveis.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações são classificadas em: Pública, Interna, Restrita e Confidencial, conforme sensibilidade e impacto.

5.1. Classificação e Tratamento

a) Pública: uso irrestrito; sem rótulo; sem exigência de criptografia.
b) Interna: uso interno; rótulo “INTERNAL”; proibir envio a domínios externos sem autorização.
c) Restrita: cifrar em trânsito e em repouso; acesso “need-to-know”; proibir armazenamento local; uso de DLP obrigatório.
d) Confidencial: cifrar de ponta a ponta quando aplicável; registro de justificativa de acesso; proibido uso de mídias removíveis; descarte seguro com evidência.

6. CONTROLES DE ACESSO

Os acessos são concedidos conforme o princípio do menor privilégio, com credenciais individuais e intransferíveis. Observam-se regras de complexidade de senhas, bloqueio após tentativas inválidas e autenticação multifator (MFA) em acessos críticos e remotos.

7. CONTROLES TÉCNICOS E PROCEDIMENTAIS

Sem prejuízo de ações específicas para proteção e prevenção de riscos identificados e avaliados pelo Compliance, serão adotadas pela ATMOSPHERE, as seguintes rotinas de prevenção e proteção:

Controle de acesso adequado aos ativos das instituições por meio da identificação, autenticação e autorização dos usuários, ou sistemas, para acesso aos ativos relevantes;

Definição de senhas de acesso a dispositivos corporativos, sistemas e rede – complexidade e autenticação de múltiplos fatores – em função da relevância do ativo acessado;

Segregação de senhas e serviços por meio de gerenciador de senhas;

Limitação de acesso, uma vez concedido, a apenas recursos relevantes para o desempenho das atividades, o qual deve ser revogado rapidamente quando necessário;

Processos de rastreamento e auditoria de eventos de login e alterações de senhas em ativos relevantes locais e remotos;

Proibição de acesso ao ambiente eletrônico corporativo (e-mail, diretórios, entre outros) por dispositivos pessoais dos Colaboradores, ressalvadas as exceções aprovadas pelo Compliance, considerando que os referidos dispositivos, nesse caso, deverão contar com todas as configurações de segurança exigidas pelo Compliance;

Realização de configurações seguras de novos sistemas e equipamentos de informação e implementação de testes periódicos quanto aos processos de segurança implementados em tais ativos;

Restrição de acesso físico às áreas com informações críticas/sensíveis;

Implementação de serviço de backup dos diversos ativos das instituições;

Criação de logs e trilhas de auditoria sempre que os sistemas permitam;

Implementação de segurança de borda, nas redes de computadores, por meio de firewalls e outros mecanismos de filtros de pacotes;

Implementação de recursos anti-malware em estações e servidores de rede, como antivírus e firewalls;

Implementação de segregação de serviços sempre que possível, restringindo-se o tráfego de dados apenas entre os equipamentos relevantes;

Impedimento à instalação e à execução de software e aplicações não autorizadas por meio de controles de execução de processos; e

Realização de diligência na contratação de serviços de terceiros, inclusive serviços em nuvem.

Medidas complementares incluem: gestão centralizada de dispositivos, políticas de atualização automática, redução de superfície de ataque, proteção contra anexos e links maliciosos no e-mail corporativo e mecanismos de prevenção de perda de dados (DLP), com relatórios periódicos de vulnerabilidades.

8. MONITORAMENTO, TESTES E AUDITORIA

Esta Política será revisada, no mínimo, a cada 12 (doze) meses após a sua publicação ou quando houver alguma nova regulamentação de certificação ou nova atividade sendo exercida.

É de responsabilidade do Suporte de Tecnologia (TI), supervisionado pelo Compliance, a criação de mecanismos de monitoramento de todas as ações de proteção e prevenção implementadas para garantir seu bom funcionamento e efetividade, considerando, no mínimo, o seguinte:

Manutenção de inventários atualizados de hardware e software, bem como verificação periódica para identificação de elementos estranhos às instituições como, por exemplo, computadores não autorizados ou software não licenciado;

Manutenção dos sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas;

Monitoramento diário das rotinas de backup, executando testes regulares de restauração dos dados;

Realização periódica de testes de invasão externa e phishing;

Realização de análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura;

Testes periódicos de planos de respostas a incidentes, simulando os possíveis cenários de ameaça; e

Análise regular dos logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos, sejam externos.

Devem ser implementados controles internos efetivos para proteção das informações da ATMOSPHERE, garantindo a sua confidencialidade, integridade, disponibilidade e norteado por esta política, com as melhores práticas de mercado e regulamentações vigentes.

A ATMOSPHERE deve comunicar seus Colaboradores sobre o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, além de seus ambientes, físicos e lógicos, para verificação da eficácia dos controles implantados e proteção de

seu patrimônio e reputação, mantendo os acessos gravados e passíveis de monitoramento, portanto, não há expectativas de privacidade em sua utilização.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre os ambientes de produção, homologação e teste.

As ameaças cibernéticas devem ser analisadas em conjunto com as vulnerabilidades detectadas por Compliance e TI nos ativos de informação e devem possuir monitoramento proativo.

9. PLANO DE CONTINUIDADE E CONTINGÊNCIA

O Plano de Continuidade e Contingência abaixo integra esta Política.

9.1. Objetivo

O presente Plano de Contingência e Continuidade de Negócios (“Plano”) tem como objetivo definir os procedimentos que deverão ser seguidos pela ATMOSPHERE, no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos.

Estratégias e planos de ação foram elaborados com o intuito de garantir que os serviços essenciais da ATMOSPHERE sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

O Plano prevê ações que durem até o retorno à situação normal de funcionamento da ATMOSPHERE dentro do contexto de seu negócio.

O Plano da ATMOSPHERE identifica duas variáveis para o funcionamento adequado da empresa: Infraestrutura e Processos.

A Infraestrutura engloba todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática e sistemas. Para cada um dos itens que compõem a Infraestrutura existe uma ação a ser tomada.

Já os processos são as atividades realizadas para operar os negócios da ATMOSPHERE. Os processos dependem da Infraestrutura toda ou de parte da estrutura em funcionamento. Somente com os processos em andamento pode-se definir que o plano de ação foi bem executado.

9.2. Estrutura Operacional

A ATMOSPHERE é uma gestora de recursos de terceiros, na forma definida pela Resolução editada pela Comissão de Valores Mobiliários n° 21, de 25 de fevereiro de 2021, de modo que precisa contar com uma estrutura operacional desenvolvida e preparada para eventuais emergências. O suporte para essa estrutura operacional é um corpo funcional capacitado com áreas de apoio, em especial em relação aos processos Suporte de Tecnologia ("TI").

9.3. Política e Procedimentos para Back-up

Diariamente todos os arquivos localizados na rede de arquivos da ATMOSPHERE são copiados, de maneira automática, para armazenamento de nuvem externo (modalidade back-up full), que armazena em real time todos os dados da operação.

Os meios de armazenamento são on-line pela Internet e com espelhamento de servidores em um local remoto.

Pela norma interna, o back-up se dará da seguinte forma:

Para a garantia do back-up das informações da ATMOSPHERE, estas devem ser armazenadas nos diretórios e pastas da rede corporativa;

Não haverá garantia de back-up para arquivos armazenados localmente nas estações de trabalho (desktops e/ou notebooks);

O back-up de dados nos servidores da rede corporativa é realizado de forma automatizada e periódico de acordo com os procedimentos de back-up e restore definidos;

O restore de dados deve ser solicitado a equipe de TI e será realizado de acordo com os procedimentos específicos;

Verificação e teste de restauração: sempre que possível, o software de back-up será configurado para verificar automaticamente o back-up. A verificação será realizada por meio da comparação do conteúdo da cópia de segurança.

9.4. Efetiva Contingência

Na impossibilidade de se utilizar o espaço físico do escritório, a ATMOSPHERE poderá continuar a funcionar por meio de home office, com notebooks autorizados, ou ainda, num local temporário de contingência, uma sala comercial alugada por dia, localizado próximo à sede, com computadores preparados com Internet rápida, além de telefones.

O acionamento das medidas de contingência descritas acima se dá com intervalo máximo de 1 (uma) hora do momento de verificação da impossibilidade de utilização do espaço físico do escritório.

A ATMOSPHERE conta com acesso remoto aos seus bancos de dados virtuais disponível a todos os colaboradores autorizados pelo Diretor de Compliance e Risco por meio do serviço de disco virtual que permite o armazenamento de arquivos em nuvem e possui aplicativos para sincronização para Windows, Mac e Android.

A ATMOSPHERE possui 02 (dois) notebooks próprios, devidamente autorizados, e com acesso à Internet móvel para qualquer eventualidade além de diferentes formas de conexão com Internet como banda-larga e wifi (rede sem fio).

O serviço de e-mail da ATMOSPHERE é garantido por parceiro que provê suporte 24/7, serviço de antispam, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A ATMOSPHERE utiliza ainda o e-mail em compatibilidade com acesso remoto de todas as mensagens pelos colaboradores.

A ATMOSPHERE conta com operadoras de telefonia. Em caso de falhas nas linhas telefônicas, os colaboradores da ATMOSPHERE ainda possuem celulares que podem substituir a telefonia fixa.

As informações do portfólio, além de estarem nos sistemas internos da ATMOSPHERE, são disponibilizadas diariamente pelas instituições administradoras dos fundos de investimentos geridos pela ATMOSPHERE, que também informará qualquer movimentação no passivo dos fundos para adequação dos seus caixas.

Em caso de falha de fornecimento de energia, a ATMOSPHERE possui nobreaks para suportar o funcionamento de seus servidores, rede corporativa, telefonia e estações de trabalho adicionais (desktops) para a efetiva continuidade dos negócios.

9.5. Estrutura de Suporte

Em caso de efetiva necessidade de utilização da estrutura de contingência, deverão ser encaminhadas para o local de contingência as pessoas responsáveis pelas funções de: boletagem das operações, de gestão das carteiras, de comunicação com as instituições administradoras e o Diretor de Compliance e Risco.

O serviço de e-mail da ATMOSPHERE é garantido por dispositivo de segurança que executa funções de firewall e antivírus.

Com seus procedimentos de back-up externo e acesso remoto a e-mails, a ATMOSPHERE pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório.

9.6. Documentação

Deverá ser mantida, em local acessível, uma lista com as informações de todos os colaboradores da ATMOSPHERE, das instituições administradoras dos fundos de investimento com as quais se realizam negócios, os clientes e os prestadores de serviços contratados.

9.7. Validação ou Testes Periódicos

Deverá ser mantida, em local acessível, uma lista com as informações de todos os colaboradores da ATMOSPHERE, das instituições administradoras dos fundos de investimento com as quais se realizam negócios, os clientes e os prestadores de serviços contratados.

10. RESPOSTA A INCIDENTES

Os incidentes de Segurança da Informação devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades da ATMOSPHERE, respeitando o nível de exposição a risco aceito e definido por ela.

a) Comunicação de Incidentes: Os Colaboradores devem comunicar imediatamente os casos de incidentes ao Diretor de Compliance e Risco. O Diretor de Compliance e Risco deve elaborar e divulgar relatório anual sobre os planos de ação e de resposta aos incidentes;

b) Tentativa de Burla: A mera tentativa de burla às diretrizes e controles estabelecidos pela ATMOSPHERE, quando constatada, deve ser tratada como uma violação;

c) Tratamento de Vulnerabilidades Identificadas: O tratamento e correções proativas das principais fragilidades ou fraquezas dos ativos de informação a serem utilizados devem estar registrados;

d) Conflitos de Interesse: A ATMOSPHERE deve possuir um processo de concessão de acessos que utiliza critérios claros e objetivos para identificar os conflitos de interesse os quais decorrem de limitações técnicas ou de situações devidamente autorizadas. Deverá haver monitoramento das atividades dos Colaboradores e das ameaças cibernéticas; e

e) Elaboração do Plano de Ação: O plano de ação deverá ser elaborado por Compliance em conjunto com TI, podendo ser envolvidos outros departamentos caso necessários para implementação das soluções para administração de eventuais contingências. Tal plano deve contar com definição expressa dos

papéis e responsabilidades na solução do impasse, prevendo acionamento dos colaboradores-chaves e contatos externos relevantes, caso aplicáveis. Deverão ser levados em consideração os cenários de ameaças previstos na avaliação de risco, havendo critérios para classificação dos incidentes, por severidade. O plano de ação deverá prever os casos de necessidade de utilização do plano de contingências nos casos mais severos, assim como o processo de retorno às instalações originais após o término do incidente. A documentação relacionada ao gerenciamento dos incidentes deverá ser arquivada para fins de auditoria.

O Plano de Contingência e Continuidade dos Negócios da ATMOSPHERE contém as diretrizes que devem orientar os processos e planejamento estratégico na disponibilidade e continuidade dos processos críticos da ATMOSPHERE.

Classificação de SLAs de Resposta

Muito Alto (Impacto Grave): interrupção ampla/risco regulatório — detecção < 1h; contenção < 4h; comunicação a partes afetadas/autoridades conforme aplicável.

Alto (Impacto Significativo): impacto relevante/setorial — detecção < 4h; contenção < 8h; comunicação ao comitê interno.

Médio (Impacto Mensurável): impacto localizado — detecção < 24h; contenção < 72h; tratamento com plano de ação.

Baixo: sem impacto material — tratamento por rotina, com registro e lições aprendidas.

11. CONSCIENTIZAÇÃO E TREINAMENTO

Programa contínuo de conscientização com treinamentos periódicos, simulações de engenharia social e comunicações regulares. A participação é obrigatória e registrada para fins de auditoria e conformidade.

12. RELATÓRIOS, REVISÃO E ATUALIZAÇÃO

A ATMOSPHERE deve possuir e manter um programa de revisão/atualização que vise garantir que todos os requisitos de segurança técnicos e legais implementados estão sendo cumpridos, atualizados e em conformidade com a legislação vigente, incluindo também a revisão periódica dos planos de ação.

A ATMOSPHERE deve prover auditorias periódicas e testes de intrusão que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

Será produzido relatório anual consolidando a implementação desta Política, os incidentes relevantes e os resultados de testes e auditorias, a ser submetido à Diretoria Executiva.

13. DISPOSIÇÕES FINAIS

Todos os colaboradores devem cumprir integralmente esta Política. O descumprimento poderá resultar em medidas disciplinares e contratuais, sem prejuízo das responsabilidades legais e regulatórias aplicáveis. Esta Política entra em vigor na data de sua aprovação pela Diretoria Executiva.