Política de Cibersegurança*

(arts. 4º, §8º, e 24, II, da Resolução CVM 21/21 e arts. 13 e 14 das Regras e Procedimentos de Deveres Básicos da ANBIMA)

*parte integrante do Manual de *Compliance* da SWM

A Política de Segurança da Informação ("PSI") visa orientar e estabelecer as diretrizes corporativas para a proteção de documentos, dados e informações ("informações") e fixar responsabilidades para todos os sócios, administradores, empregados e funcionários da SWM ("Colaboradores") e prestadores de serviços, quando a eles aplicável, que tiverem acesso ou fizerem uso de documentos, informações, sistemas, dados e recursos tecnológicos da SWM ou de seus clientes, visando seu uso adequado e responsável e sua proteção e preservação contra fraudes, danos, perda, adulteração, reprodução e divulgação ilegal. Deverá, portanto, ser cumprida e aplicada por todos os Colaboradores em todas as áreas da empresa.

IDENTIFICAÇÃO DE RISCOS (*RISK ASSESSMENT*)

A SWM mantém um Programa de Segurança Cibernética baseado em avaliação contínua de riscos internos e externos, compatível com seu porte, complexidade operacional e perfil de exposição.

Os principais ativos relevantes da SWM e riscos relacionados estão elencados na tabela abaixo:

Ativos	Riscos relacionados
Equipamentos	falhas físicas, perda, furto, acesso indevido ou uso de dispositivos pessoais não autorizados capazes de comprometer a integridade dos sistemas internos.
Sistemas	A SWM utiliza o sistema em nuvem para armazenamento de dados, documentos e informações. Nos sistemas em nuvem, os riscos concentram-se em configurações inadequadas, dependência de terceiros para manutenção e armazenamento, falhas de autenticação, indisponibilidade de serviços e vazamento de informações sensíveis.

Dados	risco de acesso não autorizado, corrupção, vazamento, exclusão acidental ou interceptação, especialmente em situações de compartilhamento inadequado.
Colaboradores	uso inadequado de informações, divulgação de senhas pessoais, compartilhamento indevido de documentos e falta de revogação imediata de acessos após desligamento, todos passíveis de resultar em incidentes de segurança com impacto operacional e reputacional relevante.

As informações geradas em decorrência da prestação de serviço de gestão de recursos de terceiros serão classificadas conforme grau de confidencialidade (informação pública, interna, restrita ou confidencial) com regras de armazenamento, transporte, compartilhamento e descarte seguro.

AÇÕES DE PREVENÇÃO E PROTEÇÃO

A SWM está comprometida e empenhada em assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, sempre com o mais alto grau de proteção de suas informações e sistemas, com programas antivírus e *firewalls* atualizados e monitorados periodicamente.

Os sistemas e computadores devem ter versões de *software* antivírus instaladas, ativadas e atualizadas permanentemente. Os recursos computacionais da SWM são protegidos contra adulterações e mantêm registros que permitem a realização de auditorias e inspeções, conforme exigência da Resolução CVM 21/21 (art. 4º, §8º).

Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Todos os Colaboradores, ao fazerem uso de qualquer Sistema da SWM, se submetem à Política de Segurança da Informação e à Política de Confidencialidade, sendo seu acesso apenas ao diretório no qual são armazenados dados e documentos disponibilizados apenas de acordo com a necessidade específica de cada usuário.

Os equipamentos de informática e comunicação, ambientes, sistemas, redes, impressoras e softwares (“Sistemas”), assim como documentos, dados e informações (“Informações”) devem ser utilizados pelos Colaboradores exclusivamente na medida do necessário à execução das suas atividades profissionais. Os ambientes, telefones, *emails*, computadores e redes da SWM poderão ser monitorados e gravados, visando garantir a integridade, confidencialidade, disponibilidade e segurança das informações utilizadas.

Toda informação produzida ou recebida pelos Colaboradores como resultado ou para fins da sua atividade profissional pertence exclusivamente à SWM ou a seus clientes, conforme o caso. Qualquer exceção deve ser explícita e formalizada por escrito.

Os documentos impressos ou copiados devem ser imediatamente retirados dos equipamentos, evitando-se que terceiros tenham acesso a tais documentos. Os documentos impressos devem ser armazenados nos locais apropriados (arquivos).

Os equipamentos, tecnologia e serviços fornecidos para o acesso à *internet* são de propriedade da SWM, que pode analisar e, se necessário, bloquear qualquer arquivo, *site*, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento da Política de Segurança da Informação.

Qualquer informação que seja acessada, transmitida, recebida ou produzida na *internet* poderá ser sujeita a monitoramento, registro e auditoria.

A SWM, ao monitorar a rede interna, pretende garantir a integridade do Sistema, dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e autorização para tal, será julgada inadequada e sujeitará o Colaborador às penalidades cabíveis. O uso de qualquer recurso para atividades ilícitas poderá acarretar sanções administrativas e legais, sendo que nesses casos a SWM cooperará ativamente com as autoridades competentes.

A SWM poderá fazer uso de dispositivos de identificação (como crachás, biometria etc.) e senhas, pessoais e intransferíveis, para proteção da identidade do Colaborador, restrição de acesso a ambientes, arquivos e documentos, tanto físicos como eletrônicos, evitando e prevenindo que uma pessoa se faça passar por outra, e garantindo a integridade e o sigilo de Sistemas e Informações Confidenciais. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto, sendo que o uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal (art. 307 – falsa identidade).

Cada Colaborador deverá ter acesso apenas aos ambientes e ao diretório no qual são armazenados dados e documentos disponibilizados apenas de acordo com sua necessidade específica, em função de suas atribuições.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, tal fato será imediatamente comunicado à Área de Tecnologia a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como a outras situações similares.

No caso de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem classificados como de maior risco, a SWM deverá assegurar que o prestador de serviços atenda aos seguintes requisitos:

(i) garantia de acesso aos dados e informações processados ou armazenados pela SWM;
(ii) confidencialidade, integridade, disponibilidade e recuperação das informações e dados processados ou armazenados pelo prestador de serviço;
(iii) aderência a eventuais certificações exigidas para a prestação do serviço contratado, caso aplicável;
(iv) provimento de informações e recursos de gestão adequados ao monitoramento dos serviços prestados;
(v) identificação e segregação dos dados de clientes, funcionários, colaboradores ou terceiros relevantes por meio de controles físicos ou lógicos; e
(vi) controles de acesso robustos para proteção de dados e informações dos clientes, funcionários, colaboradores e terceiros relevantes.

MONITORAMENTO E TESTES

Serão realizados testes anuais de segurança para os sistemas de informações, não apenas, mas em especial para os mantidos em meio eletrônico, a que tenham acesso os sócios, administradores, funcionários, colaboradores e prestadores de serviços da SWM, bem como treinamentos sobre o uso apropriado ative seguro da infraestrutura de tecnologia.

PLANO DE RESPOSTA

A SWM mantém um Plano de Resposta a Incidentes Cibernéticos que define o fluxo completo de comunicação, decisão e mitigação, conforme etapas abaixo:

Detecção: incidentes podem ser identificados por monitoramento automatizado, relato de usuários ou alerta de terceiros.

Isolamento: imediatamente após a detecção do evento, a equipe de TI deve isolar os sistemas afetados para impedir a propagação de *malware* e riscos adicionais.

Classificação: o incidente é classificado quanto à severidade (baixa, média, alta ou crítica) conforme impacto potencial e extensão da exposição.

Resposta:

- Incidentes de baixa severidade são tratados internamente pelo time de tecnologia.
- Incidentes médios e altos são encaminhados ao Conselho Consultivo.

- Incidentes críticos, quando aplicável, são comunicados ao administrador fiduciário, prestadores relevantes e reguladores (CVM/ANBIMA).

Recuperação: a área de tecnologia coordena a restauração de *backups* e retorno controlado das operações.

Acesso Remoto: é testado o acesso remoto seguro aos sistemas e documentos digitais por administradores e funcionários autorizados, com perfis restritos de acesso. O funcionamento é validado de acordo com os parâmetros definidos pela área de Tecnologia.

Verificação: Após a restauração, os sistemas são submetidos a testes de integridade, segurança e disponibilidade, garantindo que não há comprometimento dos dados.

Documentação: todos os registros de incidentes são arquivados por no mínimo 5 anos.

GOVERNANÇA

O responsável por tratar e responder a questões de segurança cibernética será indicado pelo Conselho Consultivo da SWM.

Competirá também ao Conselho Consultivo decidir sobre investimentos relacionados à segurança da informação.

A SWM mantém uma Área de Tecnologia, própria ou terceirizada, que deve seguir todas as suas políticas, normas e diretrizes, especialmente as previstas no Código de Ética e no Manual de *Compliance*, a qual possui as seguintes atribuições e responsabilidades:

- acordar sobre o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;
- testar a eficácia dos controles utilizados e informar ao Diretor de *Compliance* e Prevenção à Lavagem de Dinheiro os riscos residuais;
- configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança da informação;
- acessar arquivos e dados de quaisquer usuários, mas desde que seja estritamente necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, manutenção de computadores, realização de cópias de segurança, auditorias, testes no ambiente, apuração de fraudes ou infrações, etc., sempre mediante expressa autorização do Diretor de *Compliance* e Prevenção à Lavagem de Dinheiro;

- gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;
- administrar, proteger e testar as cópias de segurança dos programas, dados, arquivos e informações relacionados às atividades da SWM;
- planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança e disponibilidade necessárias;
- atribuir cada conta ou dispositivo de acesso a computadores, ambientes, bases de dados e qualquer outro sistema a um responsável identificável como pessoa física, sendo que:
  a) os usuários (*logins*) individuais de funcionários serão de responsabilidade do próprio funcionário;
  b) os usuários (*logins*) de terceiros serão de responsabilidade do gestor responsável pela contratação;
- proteger continuamente todos os sistemas da empresa contra código malicioso, e garantir que todos os novos sistemas só entrem para o ambiente após estarem livres de código malicioso e/ou indesejado;
- garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- realizar auditorias periódicas de configurações técnicas e análise de riscos.
- garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da SWM, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os sistemas da empresa;
- monitorar o ambiente, gerando indicadores e históricos de:
  a) uso da capacidade instalada da rede e dos equipamentos;
  b) tempo de resposta no acesso à internet e aos sistemas críticos da SWM;
  c) períodos de indisponibilidade no acesso à internet e aos sistemas críticos da SWM;
  d) incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
  e) atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);
- propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;
- propor e apoiar iniciativas que visem à segurança dos sistemas da SWM;
- analisar criticamente incidentes em conjunto com o Diretor de *Compliance* e Prevenção à Lavagem de Dinheiro;

- manter comunicação efetiva com o Diretor de *Compliance* e Prevenção à Lavagem de Dinheiro sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar as atividades da SWM.

Esta Política de Segurança da Informação (“Cibersegurança”) deve ser atualizada a cada 24 (vinte e quatro) meses, ou quando houver alteração na Regulação que demande modificações.