COMISSÃO DO MERCADO DE CAPITAIS
REPÚBLICA DE ANGOLA

GUIA DE CONSERVAÇÃO DE DOCUMENTOS PREVENÇÃO E COMBATE BRANQUEAMENTO DE CAPITAIS, FINANCIAMENTO AO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (PC/BCFTPADM)

2022-2023

COMISSÃO DO MERCADO DE CAPITAIS
REPÚBLICA DE ANGOLA

GUIA DE CONSERVAÇÃO DE DOCUMENTOS
PREVENÇÃO E COMBATE BRANQUEAMENTO DE CAPITAIS, FINANCIAMENTO AO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (PC/BCFTPADM)

Nos termos da alínea d) do artigo 8.º, conjugado com o artigo 16.º da Lei n.º 5/20[1], a obrigação de conservação consiste na preservação de evidências por 10 anos, a fim de salvaguardar, futuramente, a reconstituição de cada operação realizada. Ademais, deve-se conservar os documentos ligados à identificação e diligência, registos de transacções, as correspondências trocadas com o cliente, as comunicações à Unidade de Informação Financeira (UIF) e os resultados de análises internas.

No âmbito das acções de supervisão directa em matérias de PC/FTPADM realizadas às entidades sujeitas do Mercado de Valores Mobiliários em 2023, foram identificadas insuficiências substanciais no cumprimento da obrigação de conservação.

Neste contexto, com o intuito de garantir que as entidades sujeitas cumpram eficiente e eficazmente esta obrigação, é publicado o presente guia que aborda os aspectos necessários para a conservação dos documentos.

[1] De 27 de Janeiro, de PC/BCFTPADM.

A. Implementação de uma Política de Conservação

Uma política de conservação de documentos assegura a integridade e disponibilidade das informações relevantes, para tal é importante que apresente um fluxograma detalhado dos procedimentos de conservação, bem como a descrição detalhada dos mesmos e as equipas envolvidas em cada processo. Deve-se, ainda, designar uma equipa responsável pela gestão, revisão e implementação da política de conservação. A política de conservação de documentos deve ser adaptada às necessidades específicas das entidades sujeitas.

B. Identificação de documentos a conservar

Devem ser conservados, nomeadamente, os seguintes documentos:

- Evidências da celebração contratual com o investidor;
- Documentos de identificação pessoal do investidor ou dos representantes legais;
- Evidências da identificação do beneficiário efectivo;
- Questionários do perfil de investimento do investidor;
- Relatórios/avaliação fundamentada do risco do investidor, dos órgãos sociais, dos responsáveis com função de gestão relevante e da instituição;
- Evidências do confronto com a Lista de Sanções das Nações Unidas;
- Origem e destino dos fundos do investidor;
- Evidências da monitorização específica às Pessoas Politicamente Expostas (PPE);
- Correspondências comerciais trocadas com os investidores;
- Circuito completo das transacções efectuadas pelos investidores;
- Comunicações às autoridades competentes (Comunicações de Operações Suspeitas - COS);

- Resultados de análises internas efectuadas pelas áreas de Auditoria Interna e *Compliance*;
- Base de dados sobre a relação de investidores;
- Registos de transacções suspeitas;
- Relatórios sobre o sistema de controlo do cumprimento dos deveres;
- Relatórios de auditoria interna ao *Compliance*.
- Evidências de todos os procedimentos descritos no Manual de PC/BCFTPADM da entidade sujeita;
- Formações ministradas (contratos com entidades formadoras, conteúdo programático, bem como relação nominal e funcional dos colaboradores participantes);
- Dados históricos de incidentes/violações por parte do pessoal da entidade sujeita, bem como estatísticas sobre quaisquer medidas disciplinares tomadas contra o seu pessoal por infrações à política de *Compliance*;
- Estatísticas sobre novos clientes, negócios rejeitados ou relações comerciais extintas com base em recomendações do pessoal de *Compliance*;
- Resultados de inquéritos da direcção e pessoal sobre o grau de percepção das obrigações decorrente da lei; e
- Outros documentos relevantes relacionados com os acima identificados.

C. Formas de conservação

Os documentos devem ser adequadamente conservados em suporte electrónico ou noutros meios que permitam a sua fácil localização e acesso imediato.

D. Segurança da informação

A segurança da informação é crucial para garantir a integridade e confidencialidade dos documentos, aplicando-se a Lei que rege a Protecção de Dados Pessoais[2], sendo recomendável:

- Implementação de políticas rigorosas de controlo de acesso para assegurar que apenas usuários autorizados tenham acesso a informações sensíveis, o que ajuda a prevenir o acesso não autorizado e a manter a confidencialidade dos dados;

- Utilização de sistemas de autenticação fortes, combinando métodos como *password* e autenticação de dois factores. Esse processo adicional de verificação aumenta a segurança, tornando mais difícil para invasores comprometerem contas;

- Utilização de tecnologias de criptografia para proteger dados confidenciais durante o armazenamento e a transmissão. Isso garante que mesmo que haja uma violação de segurança, os dados permanecerão inacessíveis sem as chaves de descriptografia apropriadas;

- Manutenção de sistemas operacionais, aplicativos e *softwares* actualizados regularmente para corrigir vulnerabilidades conhecidas. Actualizações frequentes são essenciais para mitigar riscos de segurança decorrentes de falhas e brechas;

[2] Artigos 11.º (Princípio da duração do período de conservação) e 30.º (Segurança do tratamento) da Lei 22/11 de 17 Junho, sobre a Protecção de Dados Pessoais.

- Implementação de políticas de *passwords* robustas, exigindo que estas sejam fortes e actualizadas periodicamente. As *passwords* complexas dificultam a quebra por ataques, aumentando a segurança das contas;

- Realização *backups* regulares e armazenamento em locais seguros, o que permite a recuperação eficiente de dados em caso de perda, corrupção ou ataques cibernéticos;

- Manutenção do *software* antivírus atualizado e realização de verificações regulares nos sistemas, o que é essencial para identificar e neutralizar ameaças de *malwares* que possam comprometer a segurança dos sistemas; e

- Desenvolvimento e implementação de um plano de resposta a incidentes para lidar eficientemente com violações de segurança, visto que ter um procedimento claro e eficaz para responder a eventos de segurança é crucial para minimizar danos e proteger os dados da instituição.

E. Prazo de conservação

Tendo em conta que o prazo de conservação é de 10 anos, é importante que se defina procedimentos para a destruição segura dos registos quando o prazo de conservação expirar, evitando potenciais violações ou exposições indevidas.

Ao implementar esses procedimentos, a instituição assegura uma abordagem sistemática e responsável na gestão do ciclo de vida dos seus registos, contribuindo, assim, para a eficiência operacional e a conformidade legal.

F. Acções formativas

Deve-se garantir que os funcionários estejam devidamente formados e conscientes relativamente às políticas de conservação, o que envolve a implementação de acções formativas regulares, com o objectivo de assegurar que os colaboradores compreendam as políticas de conservação estabelecidas e reconheçam a importância de segui-las, sendo importante comunicar qualquer alteração à política de conservação, de forma a garantir que os funcionários estejam sempre actualizados e cumpram os procedimentos mais recentes.

G. Auditorias internas, monitoramento e actualização

Deve-se realizar auditorias internas periódicas para avaliar a conformidade com a política de conservação, bem como corrigir quaisquer não conformidades identificadas e ajustar a política conforme necessário.