

## Regras, Procedimentos e Controles Internos

A Votorantim Asset Management possui uma equipe de Compliance dedicada às suas atividades, a qual possui independência funcional da sua administração, reportando diretamente para a diretoria de Controles e Governança.

Por meio da disseminação de elevados padrões éticos como cultura organizacional e o fortalecimento dos controles em busca da conformidade, a equipe de Compliance tem a missão de desenvolver, implementar e manter programas de alto padrão para gerenciamento do risco reputacional da Instituição, além de prover assessoria aos negócios. As principais atividades desempenhadas pela área de Compliance na Asset são: (i) avaliações normativas; (ii) monitoramento de operações; (iii) acompanhamento de due diligence; (iv) detecção e reporte de conflito de interesses; (v) monitoramento de gravação de meios eletrônicos; e (vi) atendimento aos órgãos reguladores e autorreguladores.

### Controles Internos

A área de Controles Internos, subordinada a Diretoria Executiva de Controles e Governança, é a área responsável por gerir o Sistema de Controles Internos do Conglomerado Financeiro Votorantim, que está alicerçado em duas dimensões: i) Governança e o processo de gestão, envolvendo as pessoas, e ii) Metodologia e Ferramentas, meios de apoio a esse processo, tais como:

Disseminar a Cultura de Risco e Controles por meio de treinamentos e atendimentos pessoais;

- Apoiar as áreas de 1ª linha de defesa no processo de gestão dos riscos operacionais com o desenvolvimento de processos, métodos, ferramentas e políticas (RGR - Reporte Sobre a Gestão de Riscos);
- Efetuar mapeamento dos processos, identificação dos riscos e controles, além do teste de efetividade dos controles;
- Avaliar as solicitações de postergações de prazo e assunção de riscos emitindo considerações sobre o impacto de controle;
- Governança na criação ou alteração relevante de um produto ou serviço;
- Zelar pela atualização e manutenção da estrutura de normativos corporativos; e
- Acompanhar e fornecer informações para comitês e comissões relacionados ao sistema de controles internos objetivando uma efetiva gestão de riscos das áreas;

Para fins de gerenciamento de riscos da VAM, a área de Controles Internos aplica a metodologia institucional, de acordo com os requisitos regulatórios, melhores práticas e estratégia. Realiza o mapeamento das atividades, dos riscos e dos controles relacionados aos processos e registra no sistema GRC Votorantim.

Fornecer ainda os insumos para a elaboração do RGR - Reporte sobre Gestão de Riscos, conjunto de informações mínimas relacionadas ao gerenciamento dos riscos operacionais, reportadas semestralmente pelo diretor da área, no Comitê de Controles e Riscos, proporcionando aos membros do Comitê uma visão ampla, permitindo compartilhar estratégias que contribuam para uma maior eficiência e para melhores resultados no gerenciamento dos riscos das áreas e da organização.

Adicionalmente, Controles Internos acompanha os temas tratados no RGR, auxiliando na definição de planos de ação para os riscos que não se encontrem dentro do limite de tolerância da instituição.

### Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo

A política de Prevenção à Lavagem de Dinheiro estabelece diretrizes para as empresas do Consolidado Econômico Financeiro Votorantim relacionadas às práticas de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo, quais sejam:

- Prevenir a prática de lavagem de dinheiro na realização de negócios no País e no exterior, em consonância

com a legislação nacional e com a vigente em cada país onde atuamos;

- Atuamos em consonância com os compromissos internacionais assumidos pelo Governo Federal no que diz respeito à prevenção e ao combate ao crime de lavagem de dinheiro, observada a legislação vigente;
- Adotamos procedimentos, no desenvolvimento dos produtos e serviços, que objetivam inibir a prática da lavagem de dinheiro;
- Estimulamos e participamos de ações conjuntas, no âmbito do Sistema Financeiro Nacional, de prevenção e combate à lavagem de dinheiro;
- Utilizamos parâmetros estabelecidos por lei, para o registro de transações e identificação daquelas consideradas com indício de lavagem de dinheiro, no desenvolvimento ou aquisição de sistemas automatizados de monitoramento de transações realizadas;
- O Consolidado possui Comitê específico para tratar e deliberar sobre assuntos referentes à prevenção de lavagem de dinheiro e combate ao financiamento do terrorismo;
- O Consolidado mantém programas de treinamento e de disseminação de cultura de prevenção à lavagem de dinheiro e de combate ao financiamento do terrorismo, de acordo com as exigências legais e as melhores práticas do mercado;
- O Consolidado mantém estrutura responsável pelo monitoramento de todas as transações dos clientes, com foco na prevenção à lavagem de dinheiro e ao financiamento ao terrorismo. Além disso, mantém canal de comunicação destinado a receber informações de qualquer colaborador sobre operações ou propostas suspeitas identificadas na condução dos negócios;
- Avaliamos, na análise das operações, os instrumentos utilizados, a forma de realização, as partes e valores envolvidos, a capacidade financeira e a atividade econômica do cliente e qualquer indicativo de irregularidade ou ilegalidade envolvendo o cliente ou suas operações, com vistas à detecção de indício de lavagem de dinheiro;
- O Consolidado mantém armazenado cópias da documentação dos clientes, bem como registro das operações e análises de prevenção à lavagem de dinheiro realizadas mantidos de acordo com as normas internas, legislações e regulamentações dos países onde atua;
- Observamos rigorosamente as recomendações do Grupo de Ação Financeira – GAFI que especifica a lista dos países com controles insuficientes de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, bem como as listas restritivas emanadas por outros organismos internacionais de prevenção a crimes como as listas OFAC e da União Europeia; e
- O Consolidado não admite em seus negócios a movimentação de recursos por meio de contas correntes anônimas ou vinculadas a titulares fictícios.

### **Conheça seu Cliente (Know Your Customer - KYC)**

O Consolidado adota medidas de caráter restritivo quanto à realização de negócios e à manutenção de relacionamento comercial com o cliente quando as circunstâncias revelam evidências de lavagem de dinheiro. Assim, o Consolidado não se relaciona com pessoas jurídicas que sejam de instituições financeiras offshore sem presença física no país de incorporação e de emissão de licença e não afiliadas a nenhum grupo financeiro sujeito à efetiva supervisão (Shell Banks).

Não obstante, o Consolidado mantém normas específicas para a autorização de início e manutenção de relacionamento comercial com pessoas politicamente expostas, conforme exigências legais.

### **Conheça seu Parceiro (Know Your Partner - KYP)**

O Consolidado condiciona a manutenção da relação com outras instituições financeiras, parceiros ou contrapartes, à existência, no âmbito daqueles, parceiros ou contrapartes, de mecanismos relativos à prevenção ao crime de lavagem de dinheiro e de financiamento do terrorismo.

### **Conheça seu Funcionário (Know Your Employee - KYE)**

O Consolidado define e mantém normas relativas ao conhecimento de seu funcionário, com foco na prevenção e combate à lavagem de dinheiro, que incluem critérios para a contratação e verificação da conduta desses funcionários.

O Consolidado conduz, de forma sigilosa, inclusive em relação aos clientes, os processos de registro, análise e comunicação às autoridades competentes de operações financeiras com indícios de lavagem de dinheiro. Comunicamos, às autoridades competentes, as operações ou propostas de operações que, na forma da legislação vigente, caracterizem indício de lavagem de dinheiro.

### Confidencialidade

Todas as operações e acessos efetuados em meios magnéticos são registrados e passíveis de verificação a qualquer momento, independentemente de aviso prévio. O colaborador é orientado a utilizar tais informações unicamente para realização de suas atividades e de acordo com as diretrizes da Instituição, não utilizando as informações em seu próprio benefício ou em benefício de qualquer outra pessoa ou empresa. Não obstante, as áreas detentoras de informação classificadas como confidencial, restrita ou interna são passíveis de controles específicos a fim de coibir a utilização indevida da informação e auxiliar na identificação de eventuais quebras de procedimento:

- **Controles Físicos:** restringem o acesso físico às áreas (segregação física);
- **Controles Lógicos:** atuam sobre os sistemas eletrônicos e de comunicação (restrição de acesso a diretórios, e-mail externo, gravação de meios eletrônicos, entre outros);
- Controles de Conduta: Código de Conduta, manuais internos, bem como a própria regulamentação.

### Segurança da Informação

A política de Segurança da Informação é a declaração formal do Conglomerado sobre o seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, estabelecendo diretrizes e princípios gerais de segurança da informação alinhados às recomendações da ISO 27002. Descrevem todos os processos praticados de acordo com o plano estratégico definido em conjunto com a Alta Administração do Conglomerado Financeiro Votorantim e contemplam as disciplinas relacionadas à Segurança da Informação: Gestão de Acessos, Análise de Riscos e Vulnerabilidades, Tratamento de Incidentes, Monitoramento de Informações.

A Política, as normas e os procedimentos de Segurança das Informações são revisados provados por:

- Diretoria Executiva de Controles Internos
- Comitê Executivo
- Comitê de Administração

A governança e a operação na gestão da Segurança da Informação apoiam-se em processos inter-relacionados que remetem ao PDCA:

- a. Identificação
- b. Mensuração e avaliação
- c. Mitigação e Controle
- d. Monitoramento
- e. Reporte

Os dados da Organização estão armazenados digitalmente e é missão da área de Segurança da Informação manter esses dados seguros e confiáveis, desenvolvendo e aplicando soluções para garantir a confidencialidade e integridade das informações em todos os segmentos de negócios Atacado, Varejo e Corporativo.

Com foco em prevenção, a área de Segurança da Informação realiza testes de intrusão nos sites e aplicações expostos à Internet. Esses testes foram incorporados em um processo EHT (*Ethical Hacking Tests*), que é realizado anualmente, e as

vulnerabilidades encontradas são cadastradas no sistema de Gestão de Riscos Corporativo, onde são realizados follow-up dos planos de ação.

Para que possa monitorar em tempo real e apoiar os segmentos de negócios com relação ao vazamento de informação, a área de Segurança da Informação adquiriu uma ferramenta de monitoramento de eventos de segurança, com objetivo de obter maior visibilidade sobre os eventos de segurança e controle sobre a resposta a eventuais incidentes em seu ambiente. Além disso, temos uma estrutura de SOC (*Security Operation Center*) para monitoramento 24X7 de incidentes de Segurança da Informação.

## Treinamento

As ações de treinamento e desenvolvimento são realizadas pelas Escolas de Negócios Banco Votorantim e fomentam o desenvolvimento do capital intelectual, de forma alinhada às estratégias e aos valores organizacionais.

A elaboração do Programa de Treinamento e Desenvolvimento ocorre anualmente, através de levantamento das necessidades institucionais e regulatórias e disponibilidade orçamentária. As atividades de treinamento devem propiciar a elevação dos padrões de qualidade e valorização profissional, além de influenciar positivamente nos resultados individuais e do negócio.

Ao ingressar na Instituição o colaborador adere ao “Termo de Compromisso de Conduta Profissional” na sua admissão, no qual concorda em cumprir integralmente: (i) o Código de Conduta, (ii) as políticas e procedimentos para Prevenção e Combate aos Crimes de Lavagem de Dinheiro, (iii) a política de Investimentos Pessoais, (iv) as diretrizes e normas constantes da política de Segurança da Informação e (v) a Cartilha de Compliance sobre Anticorrupção, assumindo o compromisso de observá-los e aplicá-los, bem como submetendo-se às sanções previstas nas normas internas e na legislação aplicável. Não obstante, treinamentos presenciais são realizados periodicamente pelas áreas de Compliance, Jurídico, Private e Produtos. Há também um reforço desses conceitos no do treinamento obrigatório, via e-learning, do Código de Conduta