Política de Controle de Informações Privilegiadas

Melhores práticas no tratamento de informações privilegiadas

Nós, do BOCOM BBM (Conglomerado Financeiro), construímos uma relação de confiança com cada cliente e parceiro, sendo diligentes em nossa responsabilidade de manter suas informações seguras e em sigilo.

Sabemos, ainda, que uma governança sólida e bem estruturada é a primeira barreira para identificar e tratar eventuais conflitos de interesses.

Todos temos o compromisso de agir, diariamente, cientes das nossas responsabilidades e deveres na proteção dos nossos ativos, dos nossos clientes e parceiros, bem como das informações a que temos acesso.

1. Objetivo

Esta política tem por objetivo, de forma complementar ao Código de Ética e Conduta, ressaltar o nosso comprometimento em disseminar entre nossos Colaboradores e Terceiros a importância de não fazer uso inadequado de informações privilegiadas e, sobretudo, de não permitir que interesses pessoais possam se sobrepor àqueles do BOCOM BBM, de nossos investidores e clientes.

Ela busca prevenir que informações confidenciais ou privilegiadas sejam utilizadas ou acessadas inadvertidamente, de modo a proporcionar:

- Acesso linear ao mesmo nível de informação aos demais membros do mercado;
- Um tráfego mais seguro da informação dentro do BOCOM BBM; e
- O correto uso das informações pelos nossos funcionários, estagiários e pessoas de relacionamento próximo, bem como prestadores de serviço.

2. Conceitos importantes

2.1. O que é informação privilegiada?

É a informação relevante ainda não divulgada ao mercado, capaz de proporcionar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiros.

Não é permitido o uso de informações privilegiadas para nenhum propósito além daqueles que fizeram com que tais informações fossem fornecidas, tanto para Colaboradores e Terceiros, quanto para familiares ou pessoas de relacionamento próximo.

Exemplo prático: Caso a proximidade de relacionamento que um determinado Colaborador possua com uma empresa permita que ele tenha acesso a informações que influenciem a cotação de ações desta empresa, ele não poderá fazer uso dessa informação.

2.2. O que é informação confidencial?

É a informação obtida como consequência do desempenho de atividades em uma instituição, para além daquelas disponibilizadas a todos os colaboradores para uso corporativo interno, a menos que se trate de informação disponibilizada ao público ou já divulgada ao mercado (informação pública). Estão relacionadas a necessidade de sigilo e de proteção contra potenciais prejuízos financeiros ou de imagem e podem ser informações protegidas por leis específicas, como as de Sigilo Bancário e Proteção de Dados, ou ainda informações entendidas como estratégicas pela instituição ou geradas a partir de análises realizadas, podendo influenciar futuras transações.

2.3. O que é informação sigilosa?

É uma informação ou conhecimento que pode resultar em danos ao negócio ou perda de vantagem ou do nível de segurança, caso revelada (divulgada) a outros, que podem ter baixa ou desconhecida confiabilidade ou intenções indetermináveis ou hostis.

3. Diretrizes

A proteção das informações é um princípio fundamental em nosso negócio, por isso se faz necessário:

- Atuarmos sempre em defesa dos melhores interesses da Instituição, mantendo sigilo sobre nossos negócios e operações, assim como sobre os negócios e informações de nossos clientes;

- Termos ciência e estarmos em conformidade com as seguintes políticas: Código de Ética e Conduta, Política de Prevenção à Corrupção, Política de Presentes, Gratificações e Entretenimento, Política de Segurança da Informação Cibernética, Política de Boas Práticas e de Governança para LGPD, Política de Utilização de Recursos de TI, Política de Senhas e Política de Investimentos Pessoais; e

- Atuarmos conforme as boas práticas para a proteção das informações, tais como:

  i. Salvaguardar as senhas de acesso a sistemas corporativos e não compartilhar acessos;

ii. Bloquear os microcomputadores ao se ausentar da estação de trabalho, independente do intervalo de tempo;
iii. Arquivar as informações eletrônicas conforme diretrizes de armazenamento e controles de acesso; e
iv. Arquivar adequadamente as informações físicas em locais seguros; e
v. Não encaminhar informações para e-mails externos não autorizados.

A divulgação de informações à mídia utilizando o nome da nossa Instituição, mediante entrevistas ou quaisquer outras declarações, deve ser realizada somente por meio da área de Comunicação ou por profissional devidamente autorizado pela administração.

Nos reservamos o direito de vetar o uso de determinados aparelhos eletrônicos nas dependências da instituição, se o uso destes resultar em possibilidade de quebra de confidencialidade da informação.

A informação deve possuir níveis e critérios adequados de proteção que garantam a sua confidencialidade, integridade, disponibilidade, autenticidade, legalidade e auditabilidade, de acordo com a importância para a instituição, criticidade e requisitos legais. Devemos possuir a estrutura necessária para que as informações estejam suficientemente seguras, sejam elas armazenadas ou transmitidas, tais como controle de acesso físico e lógico, utilização de câmeras de segurança e segregação de funções, monitoramento contínuo, criptografia e sistemas de prevenção, para que não haja conflito de interesse.

Nós poderemos elaborar e divulgar a qualquer momento uma Lista Privilegiada (“Watch List”) que contemple o nome de empresas com as quais nossa Instituição esteja em negociação ou iniciando uma negociação, impedindo assim que nossos funcionários e pessoas de relacionamento próximo, bem como prestadores de serviço que tenham acesso a essa informação, negociem esses títulos por um período determinado.

Quaisquer dúvidas ou esclarecimentos adicionais, o Compliance Corporativo deve ser consultado.

4. Considerações Finais

4.1. Penalidades

O não cumprimento das regras descritas nesta política poderá constituir razão para advertências ou punições cabíveis.

5. Referência Interna

- Código de Ética e Conduta;
- Política de Prevenção à Corrupção;
- Política de Presentes, Gratificações e Entretenimento;
- Política de Segurança da Informação Cibernética;
- Política de Boas Práticas e Governança para a LGPD;
- Política de Utilização dos Recursos de TI;
- Política de Senhas; e
- Política de Investimentos Pessoais.

6. Das responsabilidades dessa política

Responsabilidade	Responsável
Área responsável pela gestão da política	Compliance Corporativo
A quem se aplica	Todos os nossos administradores, funcionários e estagiários ("Colaboradores"), além de prestadores de serviços que tiverem acesso às nossas informações, tanto por meio de recursos de informática, quanto por qualquer outro meio de processamento, comunicação ou armazenamento ("Terceiros").
Quem aprova	Gerente e Diretor de Compliance Corporativo

7. Controle de versões e validade da política

Esta política tem validade de **2** anos.

Esta política entra em vigor em 11/06/2025.

Versão	Data	Histórico	Autores
1.	01/09/2009	Criação do Documento	Compliance
2.	01/01/2011	Revisão	Compliance

3.	31/01/2012	Revisão	Compliance
4.	15/09/2014	Revisão	Compliance
5.	19/05/2015	Revisão	Compliance
6.	20/07/2018	Revisão	Compliance
7.	12/02/2019	Revisão	Compliance
8.	30/12/2020	Revisão	Compliance
9.	11/06/2025	Revisão	Compliance

8. Aprovações

Giuliana Marconi – Gerente de Compliance Corporativo

Luiz Augusto Maffazioli – Diretor de Compliance Corporativo