Manual de Regras, Procedimentos e Controles Internos

Elaboração: *Compliance*

Aprovação: *Compliance*/ Diretoria

Versão: 3

Código: M009

Vigente Desde: 10/2010

Última Versão: 04/2019

ÍNDICE

1. OBJETIVO

Este documento tem por finalidade definir mecanismos de controles internos para tender as diretrizes estabelecidas na IN CVM nº 558.

2. DESCRIÇÃO DA NORMA

2.1. Metodologia para Gestão de Riscos e Controles

Os processos, controles e riscos inerentes às atividades são mapeados e registrados em matrizes de riscos para facilitar o acompanhamento e o monitoramento da evolução do sistema de controles internos da instituição.

Para padronizar e otimizar o mapeamento dos riscos adotamos um Dicionário de Risco e um Dicionário de Processos a fim de estabelecer um padrão dos termos dos riscos e macroprocessos das áreas internas, de acordo com suas complexidades e com a evolução dos negócios.

O trabalho de mapeamento contempla a classificação dos riscos pelo impacto que podem gerar caso sejam concretizados, que poderá ser:

- Risco de Mercado: possibilidade de perdas decorrentes de variações de mercado, como alterações de taxa de juros, câmbio, preço de ações e commodities.

- Risco de Liquidez: possibilidade de perdas em razão da incapacidade de liquidar operações sem perda significativa de valor ou possibilidade de falta de recursos para honrar compromissos assumidos.

- Risco de Crédito: possibilidade de perda decorrente da incerteza de inadimplência de contratos de empréstimo, contrapartes de contratos ou emissões de títulos.

- Risco Operacional: possibilidade de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.

- Risco de Imagem: possibilidade de perdas decorrentes da veiculação do nome da instituição em casos de mídia negativa, seja ela procedente ou não.

- Risco Legal: possibilidade de perdas decorrentes de processos administrativos ou judiciais bem como de multas, indenizações ou penalidades proferidas por órgãos reguladores, autorreguladores ou outras autoridades.

2.2. Gestão de Conflitos de Interesse

O Grupo BR Partners considera que a divulgação e o uso indevido de informações privilegiadas são práticas condenáveis, sujeitas tanto a sanções disciplinares, no âmbito da instituição, quanto a sanções administrativas, penais e civis.

O Grupo promove uma cultura que destaca que os colaboradores têm dever fiduciário de estar atentos a conflitos de interesse potenciais ou efetivos. Além disso, os gestores juntamente com *Compliance* estão comprometidos com a adoção de medidas apropriadas para auxiliar na gestão e resolução desses conflitos.

2.2.1. Informações Privilegiadas

De modo geral, são classificadas como informações privilegiadas as informações referentes a valores mobiliários de um determinado emissor ou de um grupo de emissores que:

- Não são de conhecimento público;
- Podem influenciar no preço do valor mobiliário;
- São precisas e específicas.

A divulgação e o acesso a informações privilegiadas devem ser restritos apenas aos colaboradores e às áreas que venham a auxiliar ou participar do desenvolvimento de atividades relacionadas a essas informações. Os colaboradores que detêm informações privilegiadas estão proibidos de:

- Obter vantagem na negociação com títulos e valores mobiliários, em nome próprio ou de terceiros, vide política de Investimentos Pessoais;
- Recomendar para terceiros, ou utilizar-se dele, para negociar títulos e valores mobiliários;
- Revelar informação a terceiros sem qualquer fundamento e em decorrência da violação de termo de confidencialidade.

Os colaboradores e as áreas de negócios que tiverem acesso a essas informações devem informar prontamente à área de *Compliance* e possuem o dever de sigilo até a divulgação ao mercado.

2.2.2. Identificação de Conflitos de Interesse

Para fins de identificação de eventuais conflitos de interesses que possam surgir existem as seguintes práticas:

- O Colaborador é obrigado a divulgar suas posições de investimentos além de possuir restrições para aquisição de valores mobiliários;
- O Colaborador é obrigado a divulgar eventuais relacionamentos pessoais que possam causar conflitos de interesse;
- O *Compliance* realizará acompanhamento para verificar eventual conflito em relação a mandatos concedidos para a área de Assessoria Financeira;
- O *Compliance* é responsável por monitorar parte das mensagens eletrônicas e telefonemas das sociedades que compõem o Grupo BR Partners.

2.3. Listas

A área de *Compliance* é responsável pela centralização das informações das Listas de Observação (*Watch List*) e Restrita (*Restricted List*), bem como a divulgação para as áreas competentes.

2.3.1 Listas de Observação (*Watch List*)

Na lista de observação são inseridas as informações das operações de ofertas públicas, operações estruturadas e assessorias financeiras. As informações sobre inclusão/exclusão devem ser reportadas pelas áreas de negócios para a área de *Compliance*, a partir do contato com informação confidencial ou não pública, início da negociação com o cliente, assinatura de acordo de confidencialidade (*NDA*, *Pitch* ou *Agreement*), ou qualquer situação que caracterize conflitos de interesse.

As informações enviadas devem conter os detalhes da operação, os dados dos colaboradores participantes e o responsável pela atualização de alterações no andamento da operação.

A lista de observação não veda as operações realizadas pela Tesouraria, mas pode restringir os investimentos pessoais dos colaboradores que possuírem a informação privilegiada e/ou não pública.

2.3.2 Lista Restrita (*Restricted List*)

Na lista restrita são inseridas as informações das operações formalizadas (mandato ou contrato) e as operações que estão em processo de formalização. Não obstante, a área de *Compliance* pode inserir na lista restrita empresas listadas das quais os colaboradores detém informações privilegiadas e/ou não públicas.

A lista de observação veda a realização de investimentos pessoais dos colaboradores e as negociações da Tesouraria.

2.4. Investimentos Pessoais

Os colaboradores devem realizar seus investimentos pessoais de acordo as regras estabelecidas na política de Investimentos Pessoais.

As solicitações de investimentos e as restrições nos casos de conflitos de interesse são analisadas pela área de *Compliance*.

2.5. Barreiras da Informação

As barreiras da informação tanto físicas quanto lógicas asseguram proteção às áreas sensíveis contra os riscos legais e de imagem decorrentes do acesso, do desenvolvimento e da circulação de informações confidenciais a pessoas não autorizadas. Além disso, as barreiras de informações servem para tratar conflitos de interesse entre as áreas de negócios da instituição.

2.5.1. Barreira Física da Informação

A barreira física da informação é estabelecida por meio de segregação física das demais áreas da instituição (Banco de Investimento, Tesouraria, Gestão de Recursos de Terceiros, Mercado de Capitais e Assessoria Financeira). O controle de acesso para essas áreas de negócios é realizado via identificação funcional (crachá), permitindo acesso apenas aos colaboradores autorizados.

A área de *Compliance* é responsável pela avaliação das solicitações de acesso aos ambientes restritos, alteração de layout e realização de testes periódicos da lista de acesso para esses ambientes.

2.5.2. Barreira Lógica da Informação

A barreira lógica da informação é realizada por meio de controles nos sistemas eletrônicos e de comunicação delimitando o acesso à informação. Não obstante, além dos controles preventivos, como avaliação de solicitação de acessos aos sistemas e diretórios de rede, existem também os controles detectivos que são os monitoramentos nos sistemas de comunicação.

Para os servidores há segregação de ambientes que consiste no princípio de que uma nova versão de sistema passe pelos testes necessários para evitar incidentes no ambiente de Produção. Assim, possuímos três ambientes distintos:

Ambiente de Desenvolvimento – Local onde os desenvolvedores estão trabalhando em novas características e funcionalidades dos sistemas. Não obstante, pode ser utilizado para testes em sistemas pela área de Sistemas;

Ambiente de Homologação – Local onde uma versão candidata para subir no ambiente de produção será testada e validada pelos usuários finais. A área de Sistemas é responsável pela implementação da versão neste ambiente; e

Ambiente de Produção – Local onde o sistema efetivamente roda, sendo acessado pelos usuários finais. Apenas a área de Tecnologia tem acesso aos servidores deste ambiente.

2.6. Monitoramento de Informações

São realizados monitoramentos, por amostragem, das ligações telefônicas, dos sistemas de mensagerias (*chats*) e dos e-mails dos colaboradores alocados em ambientes com acesso restrito. Para os sistemas de mensagerias e e-mails são analisadas as mensagens filtradas, por meio de regras estabelecidas, que podem trazer potencial risco para a instituição.

Os equipamentos de impressão, fotocópia, máquinas de fax, internet, dentre outros, também são monitorados.

2.7. Presentes, Brindes e Eventos

O recebimento de presentes, brindes e eventos oferecidos por clientes, fornecedores, prestadores de serviços ou qualquer terceiro devem estar de acordo com as regras estabelecidas na Norma de Brindes e Presentes. O intuito é inibir situações conflituosas que resultem na expectativa de obter algum tipo de benefício ou vantagem em função do presente oferecido.

2.8. Atividades Externas

Os colaboradores não podem desenvolver atividades externas que possam ensejar conflitos de interesse com os negócios do Grupo. O intuito é preservar a boa reputação da instituição e evitar qualquer interferência nas atividades.

As áreas de Recursos Humanos e de *Compliance* devem ser informadas sobre a participação de colaboradores em atividades externas (ex: partidos políticos, participações societárias, associação).

2.9. Familiares

Potenciais candidatos e colaboradores do Grupo que detém parentesco com outros colaboradores, clientes, concorrentes, fornecedores, prestadores de bens e serviços e parceiros de negócios devem comunicar as áreas de Recursos Humanos e de *Compliance*.

3. Segurança da Informação

A conduta adequada à garantia da Segurança da Informação é norteada por um conjunto de regras que devem ser observadas por todos que têm acesso às informações do grupo BR Partners.

A política de Segurança da Informação do Grupo visa preservar a integridade, confidencialidade e disponibilidade das informações:

- Confidencialidade: garantir que a informação é acessível somente a pessoas

autorizadas;
- Integridade: salvaguardar a exatidão e completude da informação e dos métodos de processamento;
- Disponibilidade: garantir que os usuários autorizados obtenham acesso à informação e os ativos correspondentes sempre que necessário.

O cumprimento da política de segurança da informação é um compromisso de todos os sócios e colaboradores do Grupo que devem obedecer as seguintes diretrizes:

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
- Assegurar que os recursos colocados à disposição sejam utilizados apenas para as finalidades operacionais;
- Garantir que os sistemas e as informações sob responsabilidade estejam adequadamente protegidos em conformidade com a política vigente;
- Garantir a continuidade do processamento das informações críticas aos negócios;
- Atender às normas internas que regulamentam as atividades e o seu mercado de atuação;
- Comunicar imediatamente a área de Tecnologia caso seja identificada ocorrência ou qualquer tipo de dúvida ou incidente que possa causar algum risco às atividades.

A Tecnologia da Informação tem um papel fundamental na garantia da segurança da informação e por isso valida e homologa todos os programas e equipamentos utilizados.

3.1. Acessos Lógico e Físico

Os sócios e colaboradores possuem acesso físico e lógico liberado somente aos locais e recursos necessários ao desempenho de suas atividades.

O acesso lógico somente é realizado por meio das estações de trabalho, sendo que esses equipamentos são controlados para eliminar possíveis riscos de vulnerabilidades garantindo o cumprimento da política de utilização de softwares.

A área de Tecnologia efetua o controle de acesso, de acordo com os privilégios definidos, bem como a manutenção do cadastro dos usuários por meio da informação da área de Recursos Humanos sobre as movimentações (desligamento e transferências).

O acesso físico às dependências é controlado mediante cartão magnético e autorizado pela área de *Compliance*. Todos os ambientes operacionais possuem dispositivos de leitura de cartão, e visitantes que necessitem acesso aos locais devem obrigatoriamente ser acompanhados por um colaborador autorizado.

3.2. Senha de Acesso

As senhas são um meio comum de validação da identidade do usuário para obtenção de acesso à rede, a um sistema de informação ou a um serviço. Assim, toda senha possui caráter pessoal, secreto e intransferível.

A senha deverá ser alterada a cada 45 dias corridos, sendo que a mesma não poderá ser repetida nas próximas 6 alterações. No entanto, o usuário pode alterar a sua senha, a qualquer momento, não sendo necessário aguardar os 45 dias entre as trocas.

Para a formação da senha, o usuário deverá tomar alguns cuidados para que não seja facilmente identificada por terceiros, como nomes de cônjuges, de filhos, data de nascimento ou senha igual ao nome do usuário.

O compartilhamento de senhas é considerado como falta grave e passível de sanções disciplinares.

3.3. Correio Eletrônico

As mensagens e os documentos eletrônicos estão sujeitos às legislações específicas e o uso não controlado ou inapropriado desta ferramenta pode trazer ameaças reais, tais como:

- Criminal (devido ao uso inapropriado);
- Autoridades Regulatórias (devido ao uso inapropriado);
- Contaminação por vírus (recepção de softwares mal-intencionados);
- Quebra da confidencialidade (devido ao uso inapropriado);
- Danos a Imagem (devido ao uso inapropriado).

As caixas postais do correio eletrônico, incluindo as informações contidas em seus arquivos, são propriedade do Grupo, reservando-se o direito de monitorar e gravar toda a atividade. O uso da caixa postal de correio eletrônico e dos demais recursos de informática indica o consentimento do usuário a essa monitoração e, quando necessário, à divulgação às autoridades competentes de quaisquer evidências que possam constituir crime, delito ou violação às atividades.

3.4. Internet Corporativa

O acesso à internet deve segue políticas e normas visando proteger o Grupo contra ameaças internas e externas à segurança das informações que trafegam na Rede.

O acesso às páginas da Internet, por meio dos recursos disponibilizados, caracteriza um instrumento de trabalho e, assim destina-se e limita-se à execução das atividades pertinentes à função.

O usuário deve conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade, privacidade e proteção de propriedade intelectual. Todo acesso à internet é controlado e registrado em

sistema, dessa forma, o Grupo reserva-se o direito de examinar e de monitorar o acesso.

3.5. Software

O Grupo concede a seus sócios e colaboradores, juntamente com os servidores, desktops, notebooks e demais recursos disponíveis do seu patrimônio, a concessão de utilização de softwares, devidamente licenciados para o desempenho de suas atividades.

A área de Tecnologia é responsável por:

- Avaliar a necessidade de aquisição de softwares, bem como a sua compatibilidade;
- Proceder a instalação dos softwares adquiridos;
- Efetuar a transferência de software entre áreas ou entre computadores da mesma área;
- Manter em local apropriado e em segurança os discos originais e seus backup's (cópias de segurança), bem como os respectivos manuais e contratos de cessão de uso;
- Acompanhar, juntamente com o usuário, o prestador de serviço, quando de atualizações de software/hardware, apresentações de novos aplicativos etc.

3.6. File Server Corporativo

É obrigação do usuário segmentar e gravar os documentos sempre na pasta da área correspondente, não podendo armazenar documentos do Grupo na pasta pessoal.

3.7. Continuidade de Negócios

O Grupo possui um Plano de Continuidade de Negócios (PCN) para garantir a continuidade operacional dos processos vitais sob o impacto de um evento que venha a paralisar, total ou parcialmente, um processo crítico por um tempo maior que a tolerância à paralisação, incluindo perda ou inacessibilidade da unidade principal. Além disso, tem também por objetivo assegurar que, em caso de emergência, os processos de negócios críticos possam ser restabelecidos antes de causar prejuízos sensíveis.

Anualmente as áreas de Tecnologia, Sistemas e *Compliance*, responsáveis por atualizar todo o material do PCN, devem revisitar os processos das áreas a fim de identificar atividades não consideradas no plano de contingência que são de extrema relevância para a continuidade das operações. Durante a análise dos processos internos são também analisados os sistemas utilizados para o desempenho das atividades e quais destes são imprescindíveis para a continuidade dos negócios.

3.7.1. *Business Impact Analysis* (BIA)

A partir do mapeamento dos processos internos cada área elenca as atividades mais críticas para o bom funcionamento dos negócios e que, portanto, deverão ser contingenciadas a fim de evitar perdas caso ocorra um evento de descontinuidade de negócios. Após a identificação das atividades contingenciáveis são traçados cenários com os possíveis eventos de descontinuidade para cada uma dessas atividades de maneira a verificar o impacto da interrupção delas.

Para que se chegue ao risco de cada cenário de descontinuidade, é avaliada a reversibilidade do evento, ou seja, o prazo para se restabelecer a atividade; a probabilidade de ocorrência do evento; e a gravidade dele, isto é, o impacto gerado para as operações. A multiplicação destes fatores indica a criticidade de cada cenário para que o contingenciamento de cada um seja priorizado de acordo com o risco que representa para a organização.

3.7.2 Planos de Contingência (PC)

Os planos de contingência são os documentos em que constam todas as informações sobre cada cenário de contingenciamento, possui o prazo de identificação do evento, o prazo máximo de recuperação da atividade, os responsáveis pela comunicação, ações de prevenção, plano de contenção, plano de restabelecimento e programa de testes.

3.7.3. Estratégia

A estratégia de execução de cada plano de contingência é baseada no risco que cada cenário representa para a instituição, diferenciando ações de acesso remoto ao sítio de contingência ou deslocamento físico das pessoas responsáveis a este mesmo local.

3.7.4. Plano de Comunicação

O plano de comunicação interno prevê todos os possíveis cenários de contingência e seus respectivos responsáveis pela comunicação dos eventos, pelo restabelecimento das atividades e quais são os usuários afetados.

A diretoria do BR Partners é responsável por deliberar a respeito da comunicação ao mercado quando da entrada em contingência da organização.

3.7.5. Detecção de Eventos de Contingência

A detecção de um evento que possa resultar em uma interrupção ou desastre é de responsabilidade das áreas de TI e Sistemas ou de qualquer colaborador que perceba situações emergenciais no decorrer de suas atividades.

3.7.6. Back-up de Dados

As mídias com os back-ups diários e mensais dos bancos de dados são armazenadas com uma empresa, sob contrato com cláusulas de Acordo de Nível de Serviço (SLA), prevendo a sua disponibilização em até duas horas para a cidade de São Paulo. O transporte das mídias é feito em veículos fechados, sem identificação e são acondicionadas em malas anti-chama e anti-choque, lacradas e com controle de envio e recepção.

3.7.7. Plano de Testes

Para todo plano de contingência (PC) é criado um plano de teste com periodicidade pré-definida e factível de ser realizado pelas áreas impactadas. Os testes têm como finalidade simular reais situações de contingência para certificar o funcionamento dos processos e sistemas.

Os resultados dos testes são documentados e constantemente revisitados a fim de evitar os problemas relatados pelos testes. O teste de deslocamento de pessoas é realizado no mínimo anualmente.

4. Treinamento

As áreas de *Compliance* e de Recursos Humanos são responsáveis pela implementação, atualização e acompanhamento do programa de treinamento para todos os sócios e colaboradores do Grupo que possuem acesso a informações confidenciais.

No momento da contratação são realizados treinamentos que abrangem temas como Confidencialidade, Controles Internos, Prevenção à Lavagem de Dinheiro, Lei Anticorrupção, Responsabilidade Socioambiental, Segurança da Informação entre outros.

Os colaboradores assumem, por meio de termo de ciência e adesão, o cumprimento de todas as regras internas aplicáveis, bem como os princípios preconizados no Código de Conduta.

5. REVISÃO

Este documento deve ser revisado, no mínimo, anualmente.