Política de Regras, Procedimentos e Controles Internos da LAPB Gestão de Recursos

(11) 4550 2950 | ri@lapb.com.br
Rua Bandeira Paulista, 600 Conj. 73 |São Paulo - SP

ÍNDICE

INTRODUÇÃO

Esta Política tem como objetivo estabelecer os conceitos, regras e procedimentos dos controles internos da LAPB Gestão de Recursos ("LAPB").

A LAPB busca por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes atendendo a elevados padrões éticos e profissionais.

O Departamento de Compliance é o responsável por administrar a Política, assim como verificar a correta aderência dos colaboradores às políticas e códigos, bem como a atualização em relação às legislações em vigor e realização de testes periódicos dos processos e controles internos, efetuando as correções de quaisquer falhas detectadas. O Departamento de Compliance deve também oferecer suporte as outras áreas esclarecendo dúvidas sobre as políticas, manuais e regulamentos internos.

As políticas aqui apresentadas poderão ser atualizadas e complementadas, e é de responsabilidade de todos os colaboradores conhecer e cumprir todas as obrigações legais e regulatórias em suas atividades, prezando por altos padrões de conduta profissional. Também é obrigação de todos os colaboradoes notificar o Departamento de Compliance em casos de condutas indevidas sob o ponto de vista legal, ético ou regulatório.

ESTRUTURA

O Departamento de Controles Internos é independente e não está subordinado a nenhum outro departamento da LAPB. O Diretor de Controles Internos indicado no Contrato Social e na Comissão de Valores Mobiliários está subordinado apenas ao Comitê Executivo possuindo comunicação direta para a divulgação dos resultados decorrentes das atividades de compliance incluindo irregularidades ou falhas identificadas.

O Diretor de Compliance é o responsável pela implementação geral dos procedimentos e adesão das políticas da LAPB e normas regulamentares em vigor por todos os departamentos. Além de supervisionar as atividades dos colaboradores, o Departamento de Compliance deve oferecer esclarecimentos e suportes requisitados pelos próprios colaboradores.

O Departamento de Compliance possui autonomia e autoridade para questionar os riscos assumidos nas operações realizadas pela mesa de operações devendo ter embasamento do Departamento de Risco.

É vedado ao Diretor de Compliance a atuação em funções e atividades relacionadas à administração de recursos de terceiros e à distribuição ou consultoria de valores mobiliários. Também é vedada sua participação em qualquer atividade que limite sua independência.

CONTROLES INTERNOS

O Departamento de Compliance supervisiona a estrita obediência de todos os colaboradores ao Código de Ética. Anualmente todos os colaboradores devem preencher e assinar a Declaração Anual de Investimento e Endividamento Pessoal. Também deve haver preciso cumprimento à Política de Prevenção à Lavagem de Dinheiro e à Política de Combate ao Suborno e Corrupção.

Ocasionalmente o Departamento de Compliance deve acompanhar a rotina dos colaboradores de modo a garantir o cumprimento dos manuais e políticas internas e a devida realização de suas atividades profissionais e exata utilização dos sistemas e planilhas bem como possíveis melhorias. A supervisão dos colaboradores que desempenham funções relacionadas à administração de carteiras de valores mobiliários ainda inclui a observância de que atuem com imparcialidade evitando qualquer potencial conflito de interesse.

Caso o Departamento de Compliance verificar algum desvio ou defeito nas atividades internas da LAPB deve montar um plano de ação definindo um prazo e as melhorias a serem implementadas. Ao mesmo tempo o Departamento de Compliance deve mitigar as ocorrências de ilícitos ou atividades contrárias à regulação.

O Diretor de Compliance pode a qualquer momento requisitar a estação de trabalho de um colaborador com o propósito de efetuar exames e análises quando houver suspeitas de descumprimento dos regulamentos internos ou atividades ilegais. A solicitação do computador é válida apenas com a finalidade de averiguar a correta observância das normas internas e utilização adequada dos recursos disponibilizados pela LAPB devendo o Diretor de Compliance evitar qualquer exame que fira as regras e leis trabalhistas.

Cada colaborador possui acesso eletrônico ao servidor apenas as pastas e arquivos relacionados à sua atividade. Apenas o Departamento de Compliance e os principais executivos da LAPB que compõem o Comitê Executivo possuem acesso irrestrito aos arquivos do servidor. Eventualmente o Departamento de Compliance apura se os acessos estão adequados e sendo respeitados pelos colaboradores. Prudência maior é dada para informações confidenciais de clientes cujos dados pessoais não podem ser copiados e devem ser utilizados apenas nas dependências da LAPB. O Departamento de Compliance deve observar acessos não autorizados e investigar os motivos. O Departamento de Compliance gerencia uma ficha com a lista de pastas eletrônicas que cada colaborador tem acesso.

Os colaboradores recebem e-mails e fazem parte de grupos de distribuição relativos à suas tarefas desempenhadas na LAPB. Apenas colaboradores do Departamento Comercial, Departamento de Compliance e principais executivos recebem e-mails enviados pelos clientes com solicitações de movimentações.

Os colaboradores são responsáveis pelas suas estações de trabalho, devendo protegê-las corretamente. Senhas, acessos pessoais e informações confidenciais devem ser guardados e utilizados adequadamente e podem ser requisitados pelo Departamento de Compliance quando da necessidade de alguma inspeção.

A LAPB possui um servidor que está separado fisicamente em uma sala com acesso restrito e sistema de refrigeração. Toda rede computacional da LAPB está protegida por firewalls, antivírus e filtros de spans. Testes periódicos são feitos com propósito de avaliar possíveis vulnerabilidades e falhas nos sistemas operacionais, softwares e rede. São feitas avaliações de aplicativos e programas instalados, teste de “Ethical Hacking” (conjunto de técnicas de teste que utiliza os mesmos conhecimentos, ferramentas e metodologias utilizadas por um hacker para identificar pontos fracos dos controles existentes) e teste de penetração de rede (teste realizado por especialistas em segurança para procurar falhas no ambiente tecnológico).

O Departamento de Compliance tem acesso a todas as mensagens trocadas via e-mail e deve ficar atento quanto aqueles contendo anexos de arquivos de grandes tamanhos.

Todas as ligações telefônicas são gravadas e podem ser acessadas pelo Departamento de Compliance para esclarecer dúvidas ou quando houver suspeitas de descumprimento das políticas internas.

Diariamente são feitos dois tipos de backups dos arquivos salvos no servidor sendo um armazenado fisicamente no escritório e outro armazenado em nuvem em um local diferente do escritório da LAPB.

Áreas e departamentos com potenciais conflitos de interesse possuem atenção especial com supervisões in loco mais frequentes.

Anualmente o Diretor de Compliance deve preparar um relatório relativo ao ano civil imediatamente anterior à data de entrega contendo a conclusão dos exames efetuados e recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando necessário.

LEI DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados Pessoais (LGPDP) dispõe sobre o tratamento de dados pessoais dos cidadãos de forma a estabelecer como são coletados e utilizados a fim de proteger principalmente os direitos de privacidade.

A LAPB faz a coleta de informações de clientes restrita apenas ao necessário para a manutenção dos investimentos dos clientes e determinado pela legislação e órgãos reguladores. No entanto quando necessário para o cumprimento das Políticas de Combate a Corrupção e Política de Prevenção a Lavagem de Dinheiro a LAPB pode solicitar informações adicionais de forma a verificar a idoneidade do cliente. No limite do possível a LAPB também se atenta, para melhores práticas, a Lei de Proteção de Dados internacionais em especial a lei que rege na União Europeia sem a perda de vista que a obediência às leis brasileiras deve ser sempre prioritária.

Os dados parciais ou totais dos clientes só podem ser acessados pelos colaboradores demandados pelas suas atividades. É expressamente proibida pelos colaboradores a divulgação parcial ou total de dados pessoais dos clientes exceto quando requisitado por órgãos reguladores ou pela justiça. Também é expressamente proibido pela LAPB e seus colaboradores a negociação e venda parcial ou total dos dados pessoais dos clientes.

É permitida a utilização dos dados dos clientes de forma não individualizada para análises estatísticas desde que não seja possível através das estatísticas identificar o indivíduo originário dos dados.

INCIDENTES DE SEGURANÇA

Caso ocorra a divulgação de algum dado confidencial interno da LAPB deve verificar primeiramente a potencial extensão dos danos, deve-se avaliar a necessidade de comunicação privada ou pública do vazamento das informações, reavaliação das medidas de segurança da informação e caso necessário comunicação aos órgãos competentes.

PLANO DE CONTINUIDADE DE NEGÓCIOS

A LAPB possui um Plano de Contingência de forma a garantir a linearidade das operações, prevendo recursos alternativos e estratégias de continuidade em casos de ocorrências inesperadas. De modo a tornar efetivo o presente Plano, todos os funcionários e colaboradores da LAPB devem conhecer as práticas do Plano de Continuidade.

Uma vez identificada a interrupção de quaisquer dos recursos essenciais às atividades, os responsáveis pela área de TI devem ser imediatamente comunicados a fim de tomar as providências cabíveis nos termos do presente Plano de Continuidade de Negócios. Todos os colaboradores devem possuir os contatos telefônicos e e-mail dos responsáveis pela área de TI, de modo a possibilitar a comunicação da contingência ocorrida e a solução mais rápida do problema, ou quando não possível obter uma solução imediata, a opção do fluxo alternativo mais viável.

Em caso de falha de fornecimento de energia, a LAPB possui nobreak para suportar o funcionamento do ambiente até que o fornecimento seja reestabelecido, ou em caso de longa interrupção, a utilização do servidor de contingência em nuvem associados aos notebooks permitem a utilização da mesma infraestrutura.

Em caso de evacuação, impedimento à entrada no escritório ou incêndio com danos à infraestrutura local, os recursos de TI e todas as aplicações podem ser acessados remotamente através dos notebooks configurados especificamente para utilização da LAPB e que se encontram fora do escritório. Quando por alguma eventualidade a infraestrutura de TI localizada no Data Center ou escritório é afetada e não podem mais ser utilizados, é possível dar continuidade à operação usando o servidor de contingência em nuvem. Este servidor possui a mesma estrutura lógica do servidor em uso e com uma cópia atualizada das aplicações e arquivos da LAPB. A manutenção do fluxo de atividades é reforçada pelo acesso Web ao e-mail e acesso ao backup em nuvem, garantindo a continuidade do fluxo de atividades.

Em caso de falhas em computadores utilizados pelos colaboradores, a LAPB conta com máquinas de contingência para utilização e já previamente configuradas.

Links de internet de diferentes provedores garantem a redundância da rede e alta disponibilidade entre sistemas/informações da LAPB e clientes e fornecedores de serviços. A disponibilidade do link principal e redundante é monitorada 24/7, com alertas em casos de indisponibilidade. A rede cabeada interna e também distribuída via Wi-Fi é segregada da rede para visitantes.

Backups de arquivos, de estratégias e de modelos de negócios são realizados diariamente para um servidor de backup na nuvem de maneira automática, com criptografia em todas as pontas da comunicação para garantir a segurança dos dados, e com uma plataforma para recuperar em instantes qualquer arquivo caso necessário. Em complemento, realiza-se o backup local dos dados em discos de armazenamento externo, com a restauração de informações a partir do backup testada periodicamente.

Serviços utilizados pela equipe de gestão, tal como o “Bloomberg Professional” e “Broadcast” podem ser acessados via Mobile ou notebooks previamente configurados, sendo que esses serviços possuem seu próprio Plano de Contingência para manutenção de seu funcionamento e disponibilidade.

O acesso à rede é verificado por controle via login e senha única por usuário, com mudanças periódicas em tais acessos, podendo ser disponibilizado acesso remoto via *Virtual Private Network* (VPN) para determinados usuários.

O serviço de e-mail é garantido por parceiro terceirizado que oferece suporte 24/7, incluído serviço anti-spam, possibilidade de acesso via Web Mail e usuários administradores associados à camada extra de segurança via Two Factor Authentication.

Todas as atividades dos colaboradores são compartilhadas de forma a evitar que a ausência de um colaborador impeça as atividades rotineiras do departamento ou da LAPB. São feitos manuais dos sistemas e planilhas proprietárias utilizadas.

Em situações não previstas nos termos do presente Plano de Continuidade de Negócios e que podem afetar as atividades de departamentos específicos ou atividades da LAPB como um todo, será feita a mobilização prioritária de recursos humanos e eventuais aquisições de software ou hardware para manutenção do fluxo de operações da gestora.

POLÍTICA CIBERNÉTICA

A LAPB estabelece a presente Política Cibernética, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da organização, dos clientes e do público em geral. Considerando-se a rápida evolução das práticas e soluções de cibersegurança, exigindo constante adaptações, esta Política será atualizada e reavaliada por diretrizes e materiais adicionais ao longo do tempo.
A Política Cibernética visa garantir a confidencialidade, disponibilidade e integridade das informações, sejam elas de terceiros ou dados da própria LAPB.

- Confidencialidade: garante que as informações tratadas pela LAPB sejam restritas a um grupo restrito de usuários autorizados, impedindo a exposição de dados restritos e acessos não autorizados.

- Disponibilidade: garante a disponibilidade de informações aos usuários autorizados sempre que necessário.

- Integridade: garante a veracidade e completude das informações, de forma que elas sejam íntegras e sem alterações à dados por pessoas não autorizadas que possam efetuar modificações não aprovadas.

Toda informação relacionada às operações da LAPB, gerada ou desenvolvida nas dependências do LAPB, durante a execução das atividades de prestador de serviços de correspondente no país para a LAPB, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência.
Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada. A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da LAPB.
É diretriz que toda informação de propriedade da LAPB seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.
As diretrizes adotadas são:

a) As informações da LAPB, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;

b) As senhas são utilizadas como assinatura eletrônica e não devem ser divulgadas para todos, as senhas de acesso de estações de trabalhos deve ser compartilhamento com o Diretor de Compliance e os colegas de trabalho que exercem as mesmas atividades da mesma área de forma a evitar que as atividades da empresa sejam paralisadas caso seja necessário o acesso a uma estação sem a presença do usuário. O acesso de um colaborador a uma estação de trabalho de um colega deve ser feito pontualmente, com parcimônia e restrito a continuidade da atividade exercida no momento;

c) Acesso à dados confidenciais são restritos à determinados usuários e bloqueados com base no login de usuário. Acessos indevidos devem ser comunicados imediatamente ao Departamento de Compliance;

d) As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes;

e) Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados;

f) Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na LAPB ou para outras situações formalmente permitidas;

g) O computador disponibilizado para o usuário é de propriedade da LAPB;

h) A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função;

i) Apenas os equipamentos e software disponibilizados e/ou homologados autorizados pela LAPB podem ser instalados e conectados à rede;

j) Solicitar alterações de senha sempre que exista a possibilidade de a mesma ter sido comprometida;

k) Alterações em diretrizes de segurança do computador são bloqueadas por senha, impossibilitando a desativação do firewall, por exemplo;

l) Em caso de não funcionamento do software anti-vírus instalado em cada computador, é obrigação do usuário notificar prontamente a equipe de TI;

m) Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, e só podem ser conectados à rede Wi-Fi de visitantes, exceto em casos em que o Plano de Contingência requeira essa prática e em que exista autorização explícita do Departamento de Compliance;

n) A senha da rede de internet principal da LAPB e das respectivas camadas de segurança são mantidas de forma segura e não são compartilhadas com todos os usuários; e

o) Toda violação ou desvio, tais como instalação (intencional ou não) de vírus de informática, uso de software ilegal e tentativas de acesso à informações restritas, por exemplo, é investigada para a determinação das medidas necessárias e definição de possíveis sanções, visando à correção da falha ou reestruturação de processos e evitando que casos análogos se repitam.

TREINAMENTO

O Departamento de Compliance repassa a todos os colaboradores as políticas e manuais da LAPB de forma que todos tenham conhecimento das melhores práticas e condutas. A LAPB incentiva que todos os colaboradores busquem atualizações em suas respectivas atividades de trabalho.
Havendo necessidade, a LAPB promove treinamentos abertos aos colaboradores a respeito das melhores práticas de mercado.