Política de *Compliance* e Controles Internos

Legend

Abril de 2024

Versão: 5.0
Elaboração: Departamento Jurídico
Aprovação: Comitê Executivo
Classificação do Documento: Público

Índice

1. Abrangência e Adesão

Esta Política é aplicável a todos os colaboradores da Legend, assim considerados seus sócios, administradores, funcionários, prestadores de serviços, consultores e demais pessoas físicas e jurídicas ("Colaborador" ou "Colaboradores"). Os Colaboradores devem atender a esta Política ao ingressar na Legend ou sempre que as alterações forem consideradas pela Área de *Compliance* como relevantes e/ou demandarem obrigações adicionais aos Colaboradores, sendo obrigatória por parte de todos.

Esta Política é parte integrante das normas que guiam as relações da Legend e de seus Colaboradores, os quais, ao assinar o Protocolo de Recebimento e Leitura das Políticas Internas, concordam absolutamente com as diretrizes nela fixadas. A desobediência a qualquer das normas aqui expostas é tida como infração contratual, sujeitando seu autor às sanções cabíveis.

2. Estrutura e Responsabilidade

Cabe à Legend garantir, por meio de regras, procedimentos e controles internos adequados, o permanente atendimento à legislação, regulação, autorregulação e políticas internas vigentes.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à Legend contidas nesta Política, zelando para que todas as normas éticas, legais, regulatórias e autorregulatórias sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação ou indício de violação ao Diretor de *Compliance*.

Cabe à alta administração da Legend:

- A responsabilidade pelos controles internos e o gerenciamento dos riscos de *compliance*;
- Indicar um diretor responsável por *compliance* e controles internos[1], devendo tal profissional ter acesso a todas as informações e pessoas na Legend quando do exercício de suas atribuições;
- Aprovar, estabelecer e divulgar esta Política; e
- Garantir a efetividade do gerenciamento do risco de *compliance*.

O Diretor de Compliance deve:

- Auxiliar a alta administração a assegurar a efetividade do Sistema de Controles Internos e *Compliance* da Legend, atuando no gerenciamento efetivo de tais atividades no seu dia a dia;
- Gerenciar o Comitê de *Compliance* e o Conselho de Ética, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas;
- Designar os secretários das reuniões do Comitê de *Compliance* e do Conselho de Ética;
- Monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas.

É responsabilidade de todos os Colaboradores o cumprimento das normas legais, regulatórias e autorregulatórias aplicáveis às suas atividades, bem como de todas as normas internas da Legend.

Qualquer suspeita, indício e/ou evidência de desconformidade por eles verificada deve ser imediatamente comunicada ao Diretor de *Compliance*.

O Diretor de *Compliance* se reporta apenas à alta administração da Legend, com autonomia e independência para indagar a respeito de práticas e procedimentos adotados nas suas

[1] Com capacidade técnica e função independente das relacionadas à administração de carteiras de valores mobiliários, ou em qualquer atividade que limite a sua independência, na instituição ou fora dela.

operações/atividades, devendo acatar medidas que coíbam ou mitiguem as eventuais inadequações, incorreções e/ou inaplicabilidades.

Os controles e monitoramentos determinados nesta Política são prerrogativa exclusiva dos integrantes da Área de *Compliance* da Legend, sendo exercidos de forma autônoma e independente, com ampla liberdade de discussão e análise dos temas sob sua responsabilidade

A Área de *Compliance* é formada pelo diretor responsável e por analistas internos, que se dedicam ao exercício das atividades de cumprimento de regras, políticas, procedimentos e controles internos, incluindo o cumprimento das normas relativas ao combate e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção, e o encaminhamento, para decisão do Comitê Executivo, de análise sobre potenciais clientes e contrapartes da Legend.

3. Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

4. Escopo e atribuições do *Compliance*

A atuação do Diretor de *Compliance* tem por escopo:

4.1. Temas Normativos

- Controlar a aderência a novas leis, regulação e normas de autorregulação aplicáveis à Legend e às suas atividades, e apresentar o resultado de suas verificações no Comitê *Compliance*;
- Controlar e monitorar as licenças legais e certificações necessárias, e a sua obtenção/renovação/manutenção junto às autoridades reguladoras/autorreguladoras competentes;
- Auxiliar a alta administração da Legend no relacionamento com órgãos reguladores, e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;
- Realizar testes internos, revisões e relatórios obrigatórios nas frequências definidas nas políticas e manuais internos, bem como na legislação, regulação e autorregulação em vigor.

4.2. Boas Práticas

- Disseminar e promover as informações necessárias para o cumprimento das políticas internas e das normas legais, regulatórias e de autorregulação aplicáveis;
- Exercer seu controle, garantindo que as políticas e manuais pertinentes estejam atualizados e mantidos em diretório acessível a todos que delas devam ter conhecimento;
- Disponibilizar aos novos Colaboradores, junto com a Área de Gestão de Gente, as políticas internas aplicáveis, e coletar os termos de ciência e aderência por eles assinados;
- Estabelecer controles para que todos os Colaboradores da Legend que desempenhem funções ligadas à gestão de fundos de investimento ou de carteiras administradas atuem com independência[2];
- Garantir que os controles internos sejam compatíveis com os riscos da Legend em suas atividades[3];
- Analisar informações, indícios ou identificar, administrar e, se necessário, levar temas para análise e deliberação no Comitê de *Compliance* e/ou no Conselho de Ética.

[2] E atentem ao seu dever fiduciário para com os clientes, e que os interesses comerciais - ou aqueles de seus clientes - não desviem o foco de seu trabalho.
[3] Bem como efetivos e consistentes com a natureza, complexidade e risco das operações realizadas para o exercício profissional de administração de carteiras de valores mobiliários.

4.3. Governança

- Aprovar novas políticas internas no Comitê Executivo, ou a sua revisão, por força de mudanças na legislação, regulação ou autorregulação aplicáveis, ou ainda, de decisões internas da Legend;
- Aprovar a oferta de novos produtos e prestação de novos serviços pela Legend, a partir de *inputs* técnicos do Comitê de Investimento e Crédito;
- Atuar para que haja efetividade na segregação física de atividades conflitantes;
- Apresentar o resultado de seus controles e verificações no Comitê de *Compliance*;
- Monitorar e buscar a efetiva aplicação dos documentos de *compliance* e controles internos abaixo listados;
- Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da Legend e às demais políticas da Legend;
- Convocar, gerenciar, organizar e secretariar o Comitê de *Compliance*, registrando suas decisões em atas;
- Implementação de Regras e Guarda de Evidências – monitoramento da implementação de procedimentos, de cumprimento das normas e políticas internas, bem como de mecanismos de guarda de evidências;
- Salvaguarda de Informações - devem ser mantidos, pelo prazo mínimo de 5 (cinco) anos[4], os documentos e informações exigidos pela regulação aplicável[5].

5. Análise e Comunicação aos Órgãos Competentes

Toda desconformidade em temas de conduta pessoal e profissional - e a sua respectiva análise efetuada pelo *Compliance* - deve ser submetida ao Conselho de Ética da Legend para conclusão e deliberação dos passos a serem dados a tal respeito.

Nos casos aplicáveis de desvio da norma específica das atividades reguladas, o Diretor de *Compliance* deve comunicar o COAF no prazo de 24 (vinte e quatro) horas da verificação da respectiva ocorrência ou sua identificação.

Os demais prazos aplicáveis à Legend encontram-se previstos na lei e ou no Anexo a esta Política.

6. Segregação de Atividades

Cabe ao Diretor de *Compliance* assegurar e verificar que sejam devidamente segregadas das atividades de gestão qualquer outra atividade eventualmente desempenhadas pela Legend, que com aquelas guardem qualquer tipo de conflito, real ou potencial, em qualquer grau, aspecto, medida, tempo e/ou forma: a segregação em questão deverá se dar tanto física quanto logicamente, com restrição de acesso a dependências, sistemas, diretórios e arquivos apenas aos Colaboradores autorizados de cada área pertinente da Legend - e, se for o caso, entre estes e colaboradores de empresas de seu grupo econômico -, nos termos desta e das suas demais Políticas.

Todas e quaisquer atribuições de controle na Legend – notadamente, mas sem limitação, o próprio *Compliance* – não dependem nem estão sujeitas às suas áreas de negócios, de forma a assegurar a total autonomia de tais controles frente a cogitações de ordem de qualquer natureza, como, por exemplo, comercial e de consultoria.

[4] Ou prazo superior por determinação expressa de autoridade fiscalizadora.
[5] Bem como correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções. Os documentos e informações podem ser guardados em meio físico ou eletrônico, admitindo-se a substituição de documentos originais por imagens digitalizadas.

O bom uso de instalações, equipamentos e informações comuns é obrigatório para todos os funcionários. As estações de trabalho, incluindo as autônomas e os equipamentos portáteis, devem ter, sem exceção, senha de inicialização tendo seu acesso bloqueado após minutos de inatividade, liberado apenas com senha do usuário da própria estação.

As áreas de negócios possuem controle de acesso para garantir segurança e segregação física da área responsável pela administração de carteiras de valores mobiliários, de demais atividades conflitantes - a título de exemplo - caso sejam desenvolvidos negócios relacionados à intermediação, estruturação, distribuição de valores mobiliários ou outra atividade qualquer de cunho conflitante.

A segregação física é monitorada pela Área de *Compliance* mediante a governança e atualização da lista de pessoas com acesso a suas áreas de competência.

Com relação à segregação de informações, há procedimentos internos relacionados à confidencialidade de Informação devidamente classificada, conforme detalhado nos termos da Política de Segurança de Informação.

Como regra geral, os Colaboradores detentores de informações confidenciais, em função de seu cargo ou função, devem estabelecer barreiras de acesso a dados e informações pelos demais colaboradores cujo acesso seja dispensável.

Essas barreiras servem para atender diversos propósitos, incluindo a conformidade com leis e regulamentos que governam o tratamento e a utilização de certos tipos de informações, evitar situações que possam suscitar um potencial conflito de interesses e coibir má utilização de dados e/ou informações.

7. Contratações Internas

A admissão de um Colaborador para integrar os quadros da Legend (seja como empregado, sócio, administrador, prestador de serviço etc.) deve ser guiada pela perspectiva ética e de transparência, sob a visão do conceito “Conheça seu Empregado - *KYE*”, e não isoladamente pelo interesse profissional e/ou comercial e de resultado que esse Colaborador possa angariar para a Legend.

A Área de Gestão de Gente, responsável, pelo recrutamento e seleção de Colaboradores, deve realizar pesquisas sobre os antecedentes profissionais, especialmente para aqueles que ocuparão cargos de confiança.

Esta pesquisa deve ser realizada em elementos básicos:

Currículo: Verificar a autenticidade das informações prestadas por candidatos mediante confirmações com terceiros, de preferência obtidas de fontes e referências confiáveis, além da validação de documentos e comprovantes entregues.

Pesquisa de Antecedentes Profissionais: Identificar o perfil do Colaborador a ser contratado e avaliar se seus atributos são suficientes para a confiança necessária requerida para o cargo.

A Área de Compliance cabe realizar pesquisa reputacional, com periodicidade nunca superior a dois anos, por meio dos dados pessoais dos Colaboradores, não somente quando do início do relacionamento destes com a Legend, mas durante toda vigência de seu vínculo.

A avaliação dos Colaboradores deve ser realizada, em periodicidade anual ou em período menor se necessário, observando-se alterações significativas de comportamento e situações particulares dos empregados, como, por exemplo:

- conflitos de interesses com clientes e ou prestadores de serviços;
- alterações repentinas, e sem justificativas aparentes, no padrão de vida do Colaborador que não condizem com o cargo e respectiva remuneração auferida;
- alterações ou desvios comportamentais ou de conduta de qualquer natureza;
- realização de qualquer negócio de modo diverso ou atípico ao procedimento formal da Legend;
- superação de metas de forma inesperada ou modificação inusitada do resultado operacional do Colaborador e
- realização de qualquer negócio de modo diverso ou atípico ao procedimento formal da instituição.

A responsabilidade pela observância e cumprimento dos procedimentos ora instituídos cabe, indistintamente, a todos os Colaboradores e, em especial, aos sócios e administradores da Legend, a Área de Gestão de Gente, Área de *Compliance* e àqueles que exercem cargo de chefia.

Os Colaboradores devem contatar, a seu critério, seu superior imediato, a Área de Gestão de Gente, a Área de *Compliance* ou mesmo o Canal de Denúncia, caso tomem conhecimento das situações aqui descritas ou similares.

8. Contratações Externas

A contratação de serviços de terceiros deve ser precedida das seguintes providências:

- Análise em sistemas de *clipping* e outras investigações internas da Legend, com vistas a atestar a sua idoneidade e reputação;
- Exigência de documentos e das certidões reputadas convenientes, seguindo, quando aplicável, procedimentos semelhantes aos descritos na Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção e Conheça o seu Cliente;
- De acordo com a avaliação de conveniência dos profissionais envolvidos, solicitar a assinatura, pelos terceiros a serem contratados, de “Acordo de Não Divulgação” (*Non-Disclosure Agreement*) e
- Nos processos de negociação de qualquer contrato a ser celebrado pela Legend, o Colaborador envolvido na negociação deverá informar ao Comitê de *Compliance* sobre qualquer relacionamento familiar ou pessoal, sejam laços de amizade ou negocial, que tenha com membros do potencial contratado.

Após a contratação dos respectivos serviços, a Área de *Compliance* poderá, a seu critério, supervisionar os contratados.

O processo para contratação de terceiros poderá vir acompanhado ou não de concorrência prévia, visando a obter o melhor “custo x benefício” dos melhores prestadores de serviço do mercado. Cabe à área responsável pela contratação definir ou não se será adotado este procedimento, sendo responsável, inclusive, por dar as devidas justificativas pelo “não uso”, na hipótese de questionamento.

Qualquer eventual exceção às normas acima deverá ser reportada no Comitê de *Compliance*.

A contratação de terceiros deverá ser orientada pelas seguintes diretrizes:

- O critério principal para escolha e contratação de terceiros será a modalidade menor preço, mediante a obtenção de orçamentos em número determinado pelos Diretores responsáveis por Risco, *Compliance* e PLD para escolha do fornecedor ou prestador de serviços;

- Em casos excepcionais em que um fornecedor mais caro seja escolhido, a contratação deverá ser justificada com os outros critérios (por exemplo: prazo, qualidade, expertise, menor impacto ambiental etc.);
- Não haverá exigência de concorrência nos seguintes casos:
  - Compras e contratações para valores inferiores a R$ 5.000,00 (cinco mil reais), desde que os pagamentos não se refiram a parcelas de um mesmo serviço;
  - Quando já houver um contrato com prestadores de serviços recorrentes. Neste caso, não será necessário realizar concorrência a cada contratação ou compra;
  - Compras e contratações em casos de especialidade do fornecedor/prestador;
  - Compras e contratações em casos emergenciais, que será caracterizado devido à urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer o trabalho e que não pôde ser previsto antecipadamente.

9. Regras de Segurança da Informação e *Cyber* Segurança

As regras de segurança da informação e cibernética foram elaboradas com o objetivo de identificar e definir os princípios, conceitos e diretrizes relacionados à segurança da informação e à segurança cibernética, que deverão ser adotados por todos os Colaboradores que possuírem acesso a suas informações confidenciais (conjuntamente "Regra de Segurança").

A Regra de Segurança prevê, dentre diversas obrigações, a necessidade de os Colaboradores manterem confidenciais as informações a que tiverem acesso quando da realização de suas atividades profissionais.

A Regra de Segurança foi elaborada e deve ser interpretada em consonância com os demais manuais e políticas da Legend, e deverá ser revisada e atualizada a partir da operacionalização da Legend e sempre que for necessário incorporar medidas relacionadas a eventuais atividades e riscos novos ou anteriormente não abordados.

A estrutura da Regra de Segurança tem início nos princípios norteadores e diretrizes gerais que igualmente regem a segurança cibernética e a segurança da informação, e se desenvolve a partir da identificação e definição de contingências e procedimentos de engajamento direcionados à Regra de Segurança

9.1. Princípios Norteadores

Em linha com as melhores práticas atinentes à segurança da informação e à segurança cibernética, a Regra de Segurança considera que seus princípios norteadores básicos consistem em (i) confidencialidade, (ii) integridade, (iii) disponibilidade e continuidade e (iv) acesso controlado. Como será abordado nos itens seguintes, sua observância reflete em benefícios evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e outros problemas que possam comprometer os objetos específicos da Regra de Segurança.

- **Confidencialidade:** Proteção compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo, permitindo que sejam expostos voluntaria ou involuntariamente dados restritos e que devam ser acessíveis apenas por um determinado grupo de usuários.
- **Integridade:** Garantia da veracidade de dados, pois estes não deverão ser alterados enquanto forem transferidos ou armazenados. Ameaça à segurança acontece quando um determinado dado (físico ou não) fica exposto ao manuseio por uma pessoa não autorizada, que efetua divulgações e/ou alterações não aprovadas e sem o controle de seu proprietário (corporativo ou privado).

- **Disponibilidade e Continuidade:** Prevenção contra as interrupções das operações da Legend como um todo. Os métodos para garantir a disponibilidade incluirão um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.
- **Acesso Controlado:** O acesso dos Colaboradores a dados será restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

9.2. Diretrizes Gerais

Em consonância com os princípios norteadores acima expostos e com as funções usualmente designadas aos mecanismos de controles internos que tenham como objeto a segurança cibernética e a segurança da informação, identificamos abaixo as diretrizes gerais que devem permear os procedimentos de engajamento definidos nas Regras de Segurança:

- **Identificação/Avaliação de Riscos (*risk assessment*):** Identificar os riscos internos e externos, os ativos de *hardware* e *software* e processos que precisam de proteção.
- **Ações de Prevenção e Proteção:** Estabelecer um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles.
- **Monitoramento e Testes:** Detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.
- **Criação do Plano de Resposta:** Ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.
- **Reciclagem e Revisão:** Manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

9.3. Conceitos Específicos

A Regra de Segurança é estruturada a partir dos seguintes conceitos específicos:

- **Ambiente Físico:** dependências físicas da Legend;
- **Ambiente Lógico:** ambiente controlado, eletrônico, onde circularão e serão armazenadas informações e documentos confidenciais, *softwares* e sistemas;
- **Segregação:** garante que a informação, por meio de ambiente lógico ou físico, esteja disponível apenas para as pessoas que necessitarem do acesso àquela informação para a realização de suas atividades – conceito *need to know*.

9.4. Responsabilidades

De forma geral, caberá a todos os Colaboradores:

- Conhecer e cumprir fielmente a Regra de Segurança ora divulgada;
- Evitar situações que possam caracterizar negligência ou que estiverem diretamente violando as Regras de Segurança ou qualquer lei pertinente a ela, sob pena de sofrer sanções;
- Assegurar que os recursos tecnológicos e informações disponibilizados sejam utilizados em conformidade às políticas internas da Legend;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizadas;
- Procurar a Área de *Compliance* e/ou a Área de TI quando julgar necessário.

9.5. Comportamento Seguro e Confidencialidade

A Legend se compromete a adotar ferramentas e tecnologias de segurança da informação com o objetivo de garantir a integridade das informações e impedir:

- acesso e transmissão de informações e arquivos confidenciais a pessoas não autorizadas;
- liberação de senhas e códigos de identificação de Colaboradores e
- ocorrência de ataques cibernéticos. A Legend disponibilizará aos Colaboradores as ferramentas tecnológicas necessárias para o exercício de suas funções incluindo rede interna de arquivos com *backup* diário e sistema em *cloud*.

9.6. Classificação de Informação

A Legend classifica suas informações de acordo com o grau de confidencialidade e criticidade para seus negócios. Todas as informações precisam estar protegidas durante seu ciclo de vida, conforme aplicável: geração, manuseio, armazenamento, transporte e descarte.

- **Informações Públicas:** são aquelas destinadas ao público em geral, que poderão ser de caráter informativo. Exemplos: informações disponíveis no *website* da Legend; comunicados e apresentações institucionais destinadas aos clientes e parceiros (desde que não sejam consideradas como informações internas e/ou confidenciais).
- **Informações Internas:** são aquelas destinadas ao uso dos Colaboradores, que só deverão circular e ser compartilhadas internamente a quem tem necessidade de ter acesso (*need to know*), sob pena de gerar danos à Legend, a seus clientes ou Colaboradores. Exemplos: atas de comitês internos; relatórios internos; cartas e notificações de órgãos reguladores e autorreguladores cujo conteúdo não seja crítico para os negócios da Legend.
- **Informações Confidenciais:** correspondem a mais alta classificação de segurança para as informações que transitarem na Legend. Referem-se a informações cuja divulgação não autorizada poderia potencialmente causar danos substanciais, constrangimentos ou penalidades à Legend, seus clientes e Colaboradores. São também as informações cuja divulgação só é permitida a órgãos reguladores ou autorreguladores, Receita Federal, advogados, contadores, consultores especializados etc. As pessoas que tratarem essas informações têm a responsabilidade de protegê-las e, sempre que possível, somente divulgá-las mediante assinatura de acordos de confidencialidade. Exemplos: informação antecipada e não autorizada de operações, tais como fusões e aquisições; novos produtos e/ou serviços; informações protegidas por sigilo legal; informações societárias e/ou de remuneração dos Colaboradores etc.

9.7. Política de Acesso (Físico e Lógico)

A Legend possui sistema de controle de acesso de pessoas autorizadas às dependências do escritório por cartões magnéticos com possibilidade de utilização de *logs* e histórico de acesso, com o objetivo de garantir a segregação física das instalações, preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas; restringir o acesso a arquivos e permitir a identificação das pessoas que tenham acesso a informações confidenciais.

No ambiente lógico, a Legend conta com infraestrutura tecnológica que permite acesso por perfil de Colaborador com base no princípio da necessidade da informação para execução das atividades por ele realizadas. Além disso, cada Colaborador possui um identificador (ID de Colaborador) registrado de forma a assegurar a responsabilidade por suas ações. O sistema proprietário estará integrado e conta com ferramenta de gerenciamento de controle de acesso.

A Área de *Compliance* é responsável por aprovar a liberação e restrição de acesso aos Sistemas de Informação e a outros ambientes lógicos. Os acessos serão periodicamente revisados pela Área de TI, em conjunto com o *Compliance*.

A qualquer momento, o Colaborador que precisar ter acesso à informação ou à sistema restrito, deve solicitar a aprovação da Área de *Compliance*.

Em caso de desligamento de Colaborador, o responsável da área deverá comunicar o respectivo desligamento à Área de TI, com cópia à Área de *Compliance*, que deverá bloquear imediatamente o acesso do Colaborador a todos os documentos e sistemas da Legend.

9.8. Diretriz de Controle de Acesso

Cada Colaborador é responsável pelo uso adequado das informações que possui acesso, o que inclui as senhas de acesso aos sistemas de informações e crachás de identificação.

O acesso ao Centro de Processamento de Dados (CPD) da Legend é restrito às Áreas de TI, *Compliance* e Administrativo.

9.9. Diretriz para Senha

A senha é a chave de acesso pessoal que garantirá que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Por isso, cabem aos Colaboradores alguns procedimentos de segurança.

- Não compartilhar senha, não anotar em arquivos físicos ou de fácil acesso;
- Não utilizar códigos comuns, como próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário ou números sequenciais;
- As senhas precisarão ser diferentes entre si, como as de sites de administradores, bancos, sistemas internos e externos;
- Utilizar preferencialmente senhas distintas para uso corporativo e para uso pessoal e
- Trocar as senhas periodicamente e sempre que suspeitar de algo.

9.10. Política de Backup

A Legend conta com um *backup* local dos diretórios da rede realizado de segunda a sexta-feira com possibilidade de recuperação de até 5 (cinco) anos com restrições de datas específicas. Foi contratada uma empresa de armazenamento de mídia digital especializada para guarda dos *backups* mensais e anuais. Além das plataformas de *backup*, a Legend conta com um versionamento local de aproximadamente 30 (trinta) dias em dispositivos de *storage*. As rotinas de *backup* são validadas diariamente pela equipe de TI. São aplicados testes de *restore* mensais e anuais.

9.11. Privacidade

9.11.1. Diretriz de Utilização de *E-mail*

A Legend possui servidores de e-*mail* configurados com camadas de proteção de segurança para prevenir vírus ou a execução de códigos maliciosos. Os Colaboradores serão frequentemente orientados a utilizar o serviço de e-*mail* de forma segura. Seguem diretrizes para utilização de e-mail na Legend:

- As contas de e-*mail* pessoal são bloqueadas na rede da Legend.

- O e-*mail* corporativo deve estar ativo sempre que o Colaborador estiver trabalhando no computador.
- Não utilizar contas de e-*mail* pessoal para enviar qualquer tipo de informação confidencial ou interna.
- Ao receber e-*mails* com *links*, verificar se este corresponde ao endereço que aparece na tela. Para tanto, posicionar o ponteiro do *mouse* sobre o *link* (não clicar).
- Não abrir, em hipótese alguma, caso não tenha certeza da procedência do envio e da legitimidade do *e-mail.*

9.11.2. Diretriz de Utilização de Telefone

- **Número do Telefone do Colaborador**: A Legend disponibiliza telefones para utilização do Colaborador no desempenho de suas funções profissionais.
- **Propriedades do Número do Telefone**: O telefone disponibilizado para o Colaborador e as conversas associadas a esse número são de propriedade da Legend e, portanto, podem ser gravadas. Não deve ser mantida, portanto, expectativa de privacidade pessoal.
- **Responsabilidades e forma de uso**: Ao utilizar o telefone, o Colaborador é responsável por todo conteúdo da conversa e só deve fazê-lo para o seu desempenho profissional na Legend. É proibido utilizar o telefone para conversas que:
  - Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
  - Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
  - Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
  - Defendam ou possibilitem a realização de atividades ilegais;
  - Possam prejudicar a imagem da Legend; ou
  - Sejam incoerentes com o Código de Ética e de Conduta Profissional da Legend

9.11.3. Diretriz de Utilização de *Internet*

A Área de TI deve manter os acessos à *internet* configurados conforme previsto nesta Política.

A Área de TI deve manter bloqueados os *cloud services* (como *Dropbox, OneDrive e Google Drive*), por não ser permitido o uso desse tipo de serviço pelos Colaboradores. O compartilhamento de documentos por meio de *cloud services*, quando necessário, deve ser realizado pela Área de TI, com anuência da Área de *Compliance*.

- A instalação de *softwares* é de responsabilidade da Área de TI e bloqueada por senha.
- É proibido fazer *upload* ou *download* de *softwares* ou dados ilegais (pirataria)
- Não é permitido enviar ou fazer *download* de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.
- Não é permitido o uso de compartilhadores de informações como redes *Peer-to-Peer*, também conhecidas como redes P2P dentro da Legend, que são bloqueadas pelos serviços de *firewall*.
- A *internet* disponibilizada aos visitantes é acessível somente por uma rede de visitantes. Essa rede será totalmente segregada da rede interna da Legend e não é acessível aos Colaboradores.
- No caso de perda ou roubo de dispositivos móveis que contenham acesso ao e-*mail* corporativo, a Área de TI juntamente com a Área de *Compliance* deverão ser comunicadas imediatamente para fins de bloqueio.

9.11.4. Diretriz de Utilização da Rede Interna

A Legend possui segregação de pastas na rede interna. Cada área possui um perfil de acesso, e todos os perfis terão dois níveis de segurança - leitura e edição.

É proibido armazenar na rede arquivos de música, vídeos e fotos que não sejam de propriedade da Legend.

Dispositivos externos, como *pendrives* e HD externos não são permitidos devido ao bloqueio das portas USB dos computadores. Em caso de necessidade, a Área de *Compliance* deverá aprovar a exceção mediante solicitação do responsável da área do Colaborador solicitante.

O usuário não deve obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados à rede interna.

Computadores particulares, de Colaboradores da Legend ou de visitantes, não podem ser conectados à rede interna da empresa, salvo em situações com prévia autorização da Área de *Compliance*.

9.11.5. Outras Diretrizes

É proibido deixar papéis ou mídias removíveis da Legend contendo informações confidenciais sem o devido armazenamento (política de mesa limpa). Essas informações precisam estar guardadas em armários/gavetas com chave.

Informações confidenciais, quando impressas, devem ser imediatamente retiradas da impressora.

Os dados pessoais dos clientes da Legend devem ser tratados com o devido sigilo e cuidado, devendo ser observado o disposto na Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais. Em hipótese alguma esses dados serão fornecidos a terceiros, sem consentimento do cliente ou previsão legal.

9.11.6. Exceções Pontuais

Em caráter excepcional, e em função de suas atividades, alguns Colaboradores poderão ter acessos especiais concedidos. Nessas hipóteses, o Colaborador deverá fundamentar por e-*mail* as razões pela qual entende ser necessário o referido acesso especial, encaminhar a solicitação para a Área de *Compliance* e para o respectivo responsável pela área do colaborador. Nesses casos, o Colaborador deve manter todas as informações que tiver acesso sob sigilo e será responsabilizado no caso de eventual vazamento.

A Área de *Compliance*, depois de verificar as informações, e eventualmente consultar o responsável pela área, poderá solicitar o desbloqueio das ferramentas solicitadas junto a Área de TI ou poderá, alternativamente, escalar o assunto para decisão final do Comitê Executivo.

9.12. Gestão de Incidentes de Segurança

Qualquer suspeita de um incidente de segurança deve ser imediatamente reportada à Área de TI e à Área de Compliance. Nenhum Colaborador deve investigar por conta própria, ou tomar ações para se defender do ataque, a não ser que seja instruído para tal pela Área de TI, que está capacitada para conter as exposições, analisar os impactos e conduzir investigações, coletando evidências para possíveis ações jurídicas.

Incidentes relevantes que possam causar prejuízos financeiros ou materiais devem ser reportados ao Comitê Executivo para que delibere quais ações corretivas deverão ser tomadas.

9.13. Testes Periódicos

A Legend realiza testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades. A Área de *Compliance* e a Área de TI deverão monitorar os resultados desses testes e manter os registros em caso de falhas e violações da Regra de Segurança.

Os testes, realizados internamente, e, por prestadores de serviço, consideram:

- **Atualização constante de inventário de *hardware* e *software*, e sua regularidade de licenças e atualização tecnológica;**
- **Amplitude, cobertura e eficiência das rotinas de *backup* (evitar que desconfigurações, falhas de acesso, *login*, etc. gerem diretórios/*drivers*/máquinas que não estejam realizando *backup* de rotina);**
- **Teste de restauro regular de dados de *backup*;**
- **Tentativas de invasão, acesso com *login* e senha em máquinas desprotegidas etc.;**
- **Auditar eventos suspeitos de *login* e alteração de senha;**
- **Verificação/mapeamento de acessos locais ou remotos;**
- **Revisão e avaliação de limites de acesso, alçadas de poder, concessão de acesso e revogação;**
- **Verificação de configurações seguras de equipamentos;**
- **Verificação e auditoria de diretórios, pastas, arquivos etc. (verificando principalmente arquivos de foto, vídeo, *downloads*, acesso a *sites* suspeitos, *links* recorrentes, etc.);**
- **Revisão e diligência de prestadores de serviço terceirizados;**
- **Revisão e diligência de aplicativos e ferramentas de mercado, parceiros, prestadores de serviço em que haja troca de dados e intercâmbio constante;**
- **Verificação de contratos e nível de proteção de cláusulas de confidencialidade, requisitos de prestação de serviço, frequência de *report* e atendimento a requisitos de segurança;**
- **Outras mudanças na estrutura de tecnologia, prestadores de serviço, *hardware*, *software*, clientes, parceiros, funcionários etc. que possam expor a riscos.**

9.14. *Cyber* Segurança

Em consonância com as Diretrizes Gerais apresentadas acima, a Legend adotará procedimentos de Segurança Cibernética, listados abaixo, sendo certo que a supervisão desses procedimentos e desta Política cabem à Área de TI, com o apoio da Área de *Compliance*. A Área de *Compliance* deverá apresentar o resultado dos testes e monitoramento periódicos realizados com base nessa Política ao Comitê Executivo e ao Comitê de Risco e de *Compliance*. O Comitê Executivo e o Comitê de Risco e de *Compliance*, com base nesses relatórios, poderão propor (i) ajustes na presente Política, assim como (ii) planos de ação específicos.

9.14.1. Ações de Prevenção e Proteção

Em complemento aos procedimentos de Segurança da Informação previstos acima, ao incluir os novos equipamentos e sistemas em produção, a Legend contará com recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewall*. Da mesma maneira, monitorará o acesso a *websites* e restringirá a execução de softwares e/ou aplicações não autorizadas.

Adicionalmente, a Legend disporá de recursos para (i) realizar verificação de configurações, de modo a mitigar vulnerabilidades que possam surgir em razão da inclusão de novos equipamentos e sistemas em produção, incluindo a realização de testes prévios quando novos equipamentos e sistemas forem implementados em ambientes de homologação e de prova de conceito, (ii) implementar *anti-malware* em estações e servidores de rede, como antivírus e *firewall*, permitindo, também, a verificação do

acesso a *websites* e restrição a execução de softwares e/ou aplicações não autorizadas, bem como (iii) realizar *backup* das informações e dos diversos ativos da instituição, conforme as disposições do Plano de Continuidade do Negócio.

9.14.2. Monitoramento

Os sistemas, serviços, dados, informações disponíveis na Legend ou por esta disponibilizados, para serem usados pelos Colaboradores, não deverão ser interpretados como sendo de uso pessoal. Todos os Colaboradores deverão ter ciência de que o uso estará sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente da Legend, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (*software* e/ou *hardware*), pelas Áreas de TI, *Compliance* e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da Legend e, conforme o caso, servirá como evidência em processos administrativos, arbitrais e/ou judiciais.

A Área de TI da Legend é responsável pela elaboração de roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade, bem como por diligenciar de modo a manter inventários atualizados de *hardware* e *software*, bem como os sistemas operacionais e *softwares* de uso atualizados.

Periodicamente, a Área de TI realizará testes de segurança no seu sistema de segurança da informação e proteção de dados. Dentre as medidas, serão incluídas, mas sem se limitar:

- Verificação dos *logs* dos Colaboradores;
- Alteração periódica de senha de acesso dos Colaboradores;
- Segregação de acessos;
- Manutenção periódica de *hardwares*; e
- *Backup* diário, realizado em dispositivos de armazenamento locais e redundância em nuvem.

Sem prejuízo dos testes realizados, a Legend realizará, de tempos em tempos, simulações de ataques e respostas possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da Legend, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

Diante da dinâmica da Área de TI, sobretudo dos equipamentos utilizados, é recomendável que a Regra de Segurança seja revisada periodicamente, em prazo não superior à 12 (doze) meses.

9.14.3. Plano de Resposta

Havendo indícios ou suspeita fundamentada de descumprimento à Regra de Segurança ou evento pertinente à segurança da informação, a Área de TI deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento. Na hipótese de vazamento de informações sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater o evento identificado.

9.14.4. Ações em Caso de não Conformidade

Caso o evento pertinente à área de segurança da informação tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade. Eventos que envolverem a segurança das informações sigilosas ou que forem decorrentes de quebra de segurança cibernética deverão ser formalizados pela Área de TI perante a área de *Compliance*, que se encarregará de fazer a comunicação para deliberação do Comitê Executivo.

9.14.5. Considerações Finais

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes da Regra de Segurança não justificará desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, deverão ser consultadas as Áreas de *Compliance* e/ou TI.

A Legend está comprometida em lidar com informações pessoais não públicas sobre seus clientes, de forma responsável e transparente. Sendo assim, as políticas, controles e estruturas da Legend estarão aderentes à Lei Geral de Proteção de Dados e serão continuamente aprimorados.

10. Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios ("Plano de Continuidade") foi elaborado com o objetivo de identificar e definir os princípios, conceitos e diretrizes relacionados à continuidade de negócios, os quais deverão ser adotados por todos os Colaboradores, bem como terceirizados que possuírem acesso ao escritório, rede interna e sistemas.

O Plano de Continuidade foi elaborado e deve ser interpretado em consonância com os demais manuais e políticas da Legend, e deverá ser revisado pelas Áreas de TI e *Compliance*, a fim de incorporar medidas relacionadas a eventuais atividades e riscos novos ou anteriormente não abordados.

A estrutura do Plano de Continuidade tem início no princípio norteador que rege o prosseguimento dos negócios. Se desenvolve a partir da identificação de contingências e procedimentos de engajamento direcionados especificamente aos respectivos objetos do Plano de Continuidade.

10.1. Princípio Norteador

Em linha com as melhores práticas, o Plano de Continuidade considera que seu princípio norteador básico consiste em disponibilidade e continuidade dos negócios, representado pela prevenção contra as interrupções das operações da Legend como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à continuidade acontecem quando a informação deixa de estar acessível para quem necessita dela.

O Plano de Continuidade é um conjunto de procedimentos que objetiva, no caso de ocorrência de incidentes, manter as atividades e sistemas considerados críticos em nível de funcionamento previamente estabelecido e/ou recuperá-los no prazo previamente estabelecido.

Para identificação das posições e sistemas críticos, devem ser considerados os a seguir, no caso de interrupção do processo:

- impacto financeiro – situações em que a descontinuidade de negócios possa atingir a situação financeira e patrimonial da Legend;

- impacto legal – descontinuidade de negócios passível de gerar consequências legais à Legend e ou seus clientes e ou os Colaboradores;
- impacto de imagem – risco de a descontinuidade de negócios impactar a reputação e confiabilidade da Legend perante seus clientes;
- acidentes, casos fortuitos e força maior – risco de ocorrência de circunstâncias imprevisíveis que escapam completamente ao controle da Legend, tais como incêndios, terremotos, desastres naturais ou comoções sociais de grandes proporções, que determinem a descontinuidade de suas atividades e/ou a sua continuidade em local diverso da sua sede atual.

Os riscos são classificados conforme níveis abaixo:

- Nível 1: baixa probabilidade de ocorrência e/ou de impacto nas atividades da Legend, com monitoramento cotidiano para a sua prevenção;
- Nível 2: riscos demandantes de atenção constante, com impacto potencial médio nas atividades da Legend e necessidade de maior nível de controles preventivos;
- Nível 3: riscos que devem ser incondicionalmente evitados, com impacto relevante nas atividades da Legend, com adoção de rigorosos controles preventivos.

São exemplos de riscos de nível 3 as situações de falha de segurança/manutenção das instalações e equipamentos críticos da Legend, que têm como medidas preventivas a manutenção de extintores, *sprinklers*, detectores de fumaça e treinamento da brigada de incêndio, além da operação/instalação de *nobreaks*, *firewalls* e controles de acesso às dependências, sistemas e arquivos da Legend.

São exemplos de riscos de nível 2 a desatualização/falha de operação de *softwares*/equipamentos da Legend, cujas medidas preventivas incluem a atualização e verificação/testes de sua efetividade, seja nas dependências da Legend, seja na sua estrutura alternativa de contingência, bem como a manutenção de equipamentos para pronta reposição, operação ou substituição, de modo a sempre possibilitar a continuidade normal de suas atividades, mesmo em eventos de crise.

São exemplos de riscos de nível 1 situações não diretamente relacionadas à Legend e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas fora de seu estrito controle.

10.2. Continuidade de Negócios Responsabilidades

A Área de *Compliance* deverá se certificar da implementação do Plano de Continuidade para garantir o prosseguimento dos processos críticos da Legend em casos de eventos inesperados que afetem parcial ou integralmente a sua capacidade operacional, assegurando a realização de testes periódicos, conforme aplicáveis, que atestem sua efetividade. Este documento tem por objetivo informar, treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais.

À Área de *Compliance* caberá (i) manter este Plano de Continuidade sempre atualizado; e (ii) treinar os Colaboradores para casos de necessidade de acionamento do Plano de Continuidade.

10.3. Ações Adotadas para Mitigar Possíveis Impactos

Nosso Centro de Processamento de Dados (“CPD”), é equipado com controle de acesso, ar-condicionado dedicado, *links* redundantes de telecomunicações com operadoras distintas, *firewall*, antivírus e sistema de *backup* em localidade externa.

A Legend utiliza *no breaks* para atender o CPD e as posições de trabalho. Além disso, possui níveis consistentes de redundância, com *hard-drives* diversos, *backups* e no breaks. O *backup* é armazenado diariamente em ambiente em nuvem com redundância de provedores de internet e telefonia.

A Legend utiliza a nuvem da *Microsoft* como servidor de arquivos possibilitando assim a disponibilidade dos arquivos, mesmo em casos de incidentes, via *internet*.

O serviço de *e-mail* é armazenado em nuvem e a interface operacional do administrador pode ser acessada de qualquer lugar via *internet*. Os servidores são igualmente replicados em ambiente de nuvem, entrando em serviço automaticamente em caso de interrupção do servidor local.

O serviço de autenticação de usuários, o *Azure Active Directory*, está localizado na nuvem da *Microsoft* permitindo assim que todos os usuários sejam autenticados através da *internet*.

Os *softwares* contratados são no modelo *SaaS*, ou seja, disponibilizados via nuvem e podendo ser acessados de qualquer através da *internet*.

Os *softwares* desenvolvidos internamente são disponibilizados na nuvem da *Microsoft*, a *Azure*, possibilitando assim que sejam acessados de qualquer lugar via *internet*.

Localmente, a Legend conta com uma estrutura de contingência preparada para atender a quaisquer situações críticas que impossibilitem as áreas de negócio de exercerem suas atividades diárias, com recursos necessários e suficientes à continuidade das suas rotinas.

A realização dos *backups* das bases de dados Legend se dá conforme abaixo:

- Diariamente: *backup* completo para os servidores, armazenado por 14 dias;
- Semanalmente: *backup* completo para os servidores, armazenado por 4 semanas;
- Mensalmente: *backup* completo realizado no primeiro domingo de cada mês para os servidores, armazenado por 1 ano;
- Anualmente: *backup* completo realizado no primeiro domingo de janeiro para os servidores, armazenado por 5 ano

10.4. Ações em Caso de Não Conformidade

Os descumprimentos ao Plano de Continuidade serão submetidos ao Diretor responsável pela Área de *Compliance*, que endereçará o referido descumprimento e suas eventuais consequências ao Comitê Executivo.

11. Código de Ética e Conduta Profissional

Cabe ao Diretor de *Compliance* requerer dos novos Colaboradores a assinatura formal do Termo de Conhecimento e Aceitação ao Código de Ética e Conduta Profissional e das Políticas da Legend, até o último dia do mês subsequente à sua contratação.

12. Considerações Finais

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes desta Política não justificará desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, deverá ser consultada as Áreas de *Compliance*.

O descumprimento dos preceitos desta Política, assim como de qualquer outra ou Manual da Legend, pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão, desassociação, desligamento ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável.

A omissão diante da violação conhecida da lei ou de qualquer disposição desta Política – assim como de qualquer outra da Legend - não é uma atitude correta e constitui uma violação ao Código de Ética e de Conduta Profissional da Legend. No caso de conhecimento sobre o descumprimento a esta Política, o Colaborador deverá informar tal descumprimento a qualquer membro da Área de *Compliance*, que terá o dever de analisar e recomendar as respectivas ações corretivas para o Comitê Executivo.

Por fim, a Legend assegura que está comprometida em lidar com informações pessoais não públicas sobre seus clientes, de forma responsável e transparente. Nesse contexto, as Políticas, controles e estruturas da Legend estarão aderentes à Leis Geral de Proteção de Dados e serão continuamente aprimorados.