

9. Regras, procedimentos e controles internos

9.1 Descrever a política de seleção, contratação e supervisão de prestadores de serviços:

- PROCESSO DE RECRUTAMENTO & SELEÇÃO

O processo de recrutamento e seleção da Fortesec utilizará os princípios da Gestão por Competência e fornecerá subsídios para uma melhor relação com as áreas, permitindo avaliar o conhecimento do candidato, suas habilidades, experiências e personalidade, de acordo com vaga em questão. Como o Processo de Recrutamento exige criatividade para atrair o máximo de pessoas com o perfil desejado, a descrição detalhada do cargo, com pré-requisitos e competências necessárias, tornam-se fatores importantes para a adequação das expectativas dos candidatos, dimensionando suas capacidades e interesses à necessidade do trabalho a ser executado.

A área de Recursos Humanos adotará a seguinte diretriz:

- Após o recebimento do formulário de solicitação de vaga, o RH entrará em contato com o gestor para alinhar o perfil e expectativa de retorno. Dependendo das especificidades da vaga, o processo de recrutamento será realizado com o auxílio de consultoria externa.
- Os candidatos identificados passarão por entrevistas prévias e/ou realização de testes ministrados pela área de Recursos Humanos, que encaminhará ao gestor um registro detalhado do candidato. Os candidatos finalistas serão entrevistados pelo gestor requisitante da vaga, que deverá encaminhar uma resposta positiva ou negativa para a área de Recursos Humanos.
- Os candidatos aprovados serão comunicados pela área de Recursos Humanos, que acompanhará o devido aceite e admissão. Os candidatos reprovados receberão um comunicado de agradecimento pela participação no processo.

- CONTRATAÇÃO E SUPERVISÃO DE PRESTADORES DE SERVIÇOS

A Securitizadora contrata ou pode vir a contratar prestadores de serviços terceirizados para a realização de atividades como, por exemplo, empresas de auditoria, agente fiduciário, agência classificadora de risco, banco escriturador, dentre outros.

A escolha e contratação de fornecedores e prestadores de serviços devem ser baseadas em critérios técnicos, imparciais e de acordo com as necessidades da Securitizadora e suas emissões.

A política de contratação de prestadores envolve a obtenção de 3 (três) cotações de contrapartes reconhecidas em seu ramo de atuação em caso de contratos superiores ao

valor de R\$25.000,00 (vinte e cinco mil reais) anuais.

Para demandas altamente específicas, é admitida exceção a essa regra, desde que previamente justificada e aprovada pela Diretoria.

As checagens são, em sua maioria, as mesmas aplicáveis no contexto de *Know Your Client* para tomadores e têm foco em reputação, à lavagem de dinheiro e cumprimento de normas e anticorrupção.

Adicionalmente, a Securitizadora tem como boa prática fazer diligência ou pedir evidências de contrapartes de negócio a fim de confirmar se estas cumprem, adequadamente, as obrigações regulatórias que lhes cabem no contexto de operações ou relacionamento com a Securitizadora. Assim, preza-se por contrapartes com robustos procedimentos de PLDFTP, anticorrupção, dentre outros processos eventualmente aplicáveis.

Excepcionalmente, a critério da Diretoria, o processo de diligência pode ser dispensado ou simplificado na hipótese de: (a) a contraparte já ser aderente às melhores práticas aplicáveis a seu setor, bem como fiscalizada por autorregulador, (b) se tratar de contraparte reconhecida no mercado, e (c) em seu contexto regulatório, a contraparte está sujeita a diligências e fiscalizações ainda mais complexas por seus reguladores. Para fins do subitem, considera-se, em especial, eventual adesão ao Código Anbima de Melhores Práticas aplicável à atuação da contraparte.

As nossas Políticas, Manuais e Códigos detalham todos os procedimentos para as nossas contratações, observando: *Know Your client*, *Know your Supplier*, *Know your customer*, *Know your partner*.

9.2 Descrever a política de negociação de que trata o art. 17, VI, da Resolução:

Segundo a Política de Negociação de Valores da Securitizadora, é vedado às Pessoas Sujeitas, por si ou por intermédio de terceiros, negociar valores mobiliários de emissão da Fortesec, a exemplo dos certificados de recebíveis imobiliários (CRI) ou do agronegócio (CRA), no mercado primário e secundário.

Sem prejuízo da vedação acima, a negociação de outros valores mobiliários de titularidade das Pessoas Sujeitas durante o período das atividades profissionais ficará autorizada desde que não prejudique a condição dos trabalhos vinculados à Fortesec, com base no julgamento dos gestores das áreas da Fortesec.

Caso no momento de ingresso na Fortesec, as Pessoas Sujeitas já possuam os ativos restritos pela regra geral, ou ainda, venha os possuir em momento posterior, em razão de

fato fora de seu controle, por exemplo, sucessão hereditária, é necessário listá-los por meio do Termo Adicional – Declaração de Conflito de Interesses ou Desenquadramento, que se está descrito na Política de Negociação de Valores Mobiliários.

Por decisão da Alta Administração da Fortesec, fica vedado às Pessoas Sujeitas, por si ou por intermédio de terceiros, negociar no mercado primário e secundário, títulos de certificados de recebíveis imobiliários (CRI) ou do agronegócio (CRA) emitidos pela Fortesec.

Caso as Pessoas Sujeitas sejam colaboradores, fica vedada a negociação no período de 15 (quinze) dias que anteceder a data da divulgação de fatos relevantes, informações financeiras, contábeis bem como de qualquer natureza do patrimônio separado exigida pela legislação e regulamentação aplicáveis.

Além disso, a Securitizadora observa de perto assuntos relacionados a divulgação de informações confidenciais ou a utilização de informações privilegiadas na negociação de valores mobiliários, baseada no conhecimento de informações relevantes que ainda não são de conhecimento público, com o objetivo de auferir lucro ou vantagem no mercado, é crime, vez que dizem respeito a dados financeiros e aos ativos que serão lastro de operações de securitização.

Qualquer violação à Política de Negociação de Valores mobiliários será submetida ao Diretor de Riscos, *Compliance* e PLD/FTP e aos Diretores da Securitizadora.

9.3 Descrever os mecanismos de controle de informações confidenciais a que tenham acesso seus administradores, empregados e colaboradores, assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.

Introdução

Os sócios, diretores e colaboradores da Securitizadora estão sujeitos às regras de Segurança da Informação previstas nas Políticas da Securitizadora, que determina, em linhas gerais, o que segue abaixo.

O acesso a dados de operações é baseado na regra *need to know*.

De modo geral, as informações deverão ser classificadas em:

- (a) Públicas: sem restrição de acesso, tais como dados que devem ser divulgados nos termos da regulamentação vigentes.

- (b) Uso Interno: acessível a todos os Colaboradores Fortesec, tais como as políticas e manuais.
- (c) Confidencial: acessível a grupo restrito de Colaboradores, com base no princípio *need to know*, tais como clientes em fase de prospecção pela área comercial.
- (d) Secretas: informações altamente estratégicas, em fase de discussão restrita, geralmente acessadas pelas pela Diretoria.

Recursos Tecnológicos

A Securitizadora se utiliza, ainda, de estrutura tecnológica para a segregação de acessos e pastas específicas, em linha com as regras de Conflito de Interesses, Confidencialidade e Informações Privilegiadas previstas nas Políticas da Securitizadora.

Cada Colaborador é integralmente responsável pelo uso e guarda de suas senhas e login de acesso a sistemas, sites, bancos, redes, pastas, etc. Logins e senhas são de uso pessoal e intransferível.

Qualquer ação em ambientes que exijam credenciais com senha será de responsabilidade do “usuário logado”, independentemente de quem de fato operou tal ato. Por conta disso, é vedado o compartilhamento de senhas entre os Colaboradores.

Repositórios

Todos os documentos e informações confidenciais são armazenados em dois repositórios em nuvem:

- **Repositório 1:** Cada equipe da Securitizadora possui um repositório privado com uma biblioteca de documentos compartilhada, por padrão, apenas entre os colaboradores da área e Diretoria. Algumas pastas e *sites* são compartilhados com colaboradores de outras áreas, mediante política de *need-to-know* desenvolvida pela área de *Compliance*.
- **Repositório 2:** Cada colaborador possui acesso a um repositório particular vinculado ao seu usuário/*e-mail* corporativo. Nenhum outro colaborador possui acesso direto a esses arquivos, exceto quando compartilhado pelo dono.

Controle de Acesso

O controle de acesso é garantido mediante ingresso e permanência do usuário em grupos de segurança gerenciados em uma base de dados que abarca um conjunto de serviços que conectam usuários com recurso da rede que necessitem para execução de suas funções. Apenas a equipe de suporte (interna e terceirizada) possui privilégios para alterar essa configuração.

Compartilhamento de Arquivos

O compartilhamento interno é feito utilizando os dois repositórios citados acima com bloqueio de compartilhamento para fora do domínio da Securitizadora. Para compartilhamento externo, as áreas possuem uma central de compartilhamento isolada dos repositórios internos com obrigatoriedade da especificação da pessoa que terá acesso ao arquivo ou diretório específico, mediante autenticação de *e-mail* e/ou senha.

Política de Segurança

Os recursos de nuvem descritos nesse item são fornecidos pela *Microsoft* sob a égide dos principais padrões internacionais de segurança e privacidade. Principalmente, mas não de forma exclusiva:

- Autenticação *Multifactor* (MFA) obrigatória para todos os usuários.
- Proteção contra *ransomwares* e ameaças ocultas em anexos de e-mails e *link*.
- Restrição de acesso do usuário, bem como de cópia, abertura e edição de documentos em dispositivos sem conformidade com as políticas internas

9.4 Descrever os planos de contingência e continuidade de negócios:

Os documentos da Securitizadora preveem as orientações gerais abaixo, classificadas por diferentes cenários de contingências, a serem adotadas para fins da continuidade dos negócios da Securitizadora.

1. Atividades Críticas de Plano de Continuidade de Negócios

Em cenários atípicos, tais como greves, pandemias, perda de servidores ou não existência de Colaboradores suficientes para o desempenho de suas funções, a Securitizadora tem como premissa reduzir sua atuação à prática de atividades tidas como realmente críticas, que devem ser definidas por cada diretor, no âmbito da atuação de sua equipe e posteriormente validada em conjunto pela Diretoria da Securitizadora.

Após listar as atividades críticas, cabe a cada Diretor, com o apoio do time de TI, redigir plano

de continuidade de negócios de sua área.

O plano de continuidade de negócio de cada área deve considerar:

- a. Os cenários propostos que permitem aos Diretores refletir sobre táticas e estratégias para continuar suas atividades diante de indisponibilidade se dificuldades distintas;
- b. Definição do risco de se deixar de executar referia atividade crítica por algumas horas ou dias, de modo a auferir a real criticidade da atividade;
- c. Os colaboradores que, em princípio, serão designados para atua em contingência.

A definição de atividades críticas e colaboradores que retornam primeiro às suas atividades não é de modo algum relacionada a cargo ou hierarquia interna, mas assim em conforme a necessidade operacional.

2. Decretação de contingência de Negócios

A Decretação de contingência deve ser efetuada pelo Diretor de Securitização e, em sua ausência, por qualquer dos demais Diretores.

3. Cenários de Contingência

Cenário I - Ausência de estrutura de Tecnologia - *Disaster Recovery*

Todos os sistemas e aplicações utilizados na Securitizadora estão hospedados em estruturas dos respectivos fornecedores das soluções (data centers, nuvens privadas, dentre outros), que possuem alta disponibilidade operacional (24x7). Em caso de indisponibilidade desses ambientes, será acionado o plano de *Disaster Recovery*, isto é, recuperação de desastres tecnológicos, dessas empresas.

Cenário II - Impossibilidade de Acesso a Edifício

Em caso de impossibilidade de acesso aos edifícios (exemplo, inundação ou chuvas fortes), os Colaboradores com função crítica executarão tais funções de modo remoto. A Securitizadora disponibiliza para seus Colaboradores em um ambiente online todos os recursos que possuem no escritório físico, isto é e-mail, sistema de arquivos de escopo interno da Securitizadora e externo (relação com clientes, investidores e mercado), mensagem instantânea e reuniões online, entre outros. Todos esses recursos estão disponibilizados na plataforma *Office 365 Business Premium da Microsoft*.

Cenário III - Indisponibilidade de Colaboradores

Hipoteticamente, é possível que diante de alguns cenários, haja número de Colaboradores muito inferior ao necessário para que a Securitizadora execute todas as suas rotinas - exemplo, excesso de Colaboradores doentes. É responsabilidade de cada gestor de área treinar seus times de modo a garantir que haja sempre um colaborador apto a executar a rotina e as atividades de outro ("*backup*"), mitigando, assim, o risco de, em um evento crítico, alguma rotina essencial não ser rodada.

9.5 Descrever as políticas, as práticas e os controles internos para o cumprimento das normas específicas previstas no art. 19 da Resolução.

A Securitizadora disponibiliza uma Política específica de Política de Controles Internos detalhando as práticas a serem adotadas para garantir a conformidade com as normas vigentes, a ética e boas práticas de mercado.

Destaca-se a atuação do Diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Resolução CVM 60 ("Diretor de Riscos, Compliance e PLD/FTP"), com o treinamento periódico de colaboradores e gestores nesse sentido e políticas de resolução de eventuais conflitos de interesse, tendo o Diretor de Riscos, Compliance e PLD/FTP autonomia para garantir a conformidade plena da Securitizadora, não se subordinando a qualquer outro órgão da Securitizadora ou de seu grupo econômico no exercício de tal função.

São tomadas, ainda, medidas para evitar a contratação de colaboradores ou gestores que venham a representar conflitos de interesse ou risco de infração, com todas as contratações ficando sujeitas a análise prévia de condições preexistentes ou eventuais que gerem riscos, com aprovação do Diretor de Riscos, Compliance e PLD/FTP da Securitizadora para as contratações após conclusão da análise de conformidade.

O Diretor de Riscos, Compliance e PLD/FTP conta com equipe de colaboradores dedicados a manter o cumprimento das disposições legais e regulatórias, sendo que a equipe de Compliance da Securitizadora goza de extensão da autonomia do Diretor de Riscos, Compliance e PLD/FTP para o exercício de tais funções. Tal equipe é destacada das responsáveis por outras atividades exercidas pela Securitizadora, de modo a mitigar potenciais conflitos de interesse e *disclosure* de informações privilegiadas/sigilosas.

A Securitizadora é sujeita, ainda, a auditoria independente exercida por auditor devidamente autorizado em regime anual, em cumprimento às disposições legais sobre o tipo de atividade que exerce.

As informações confidenciais são segregadas de acordo com critério da equipe de

Compliance, com suporte da área de Tecnologia da Informação para estabelecer restrições de acesso a informações que poderiam gerar infrações ou conflitos de interesse.

9.6 Descrever as políticas, as práticas e os controles internos para o cumprimento das normas específicas previstas no art. 43 da Resolução, caso decida atuar na distribuição de títulos de securitização de sua emissão.

Não aplicável – A Securitizadora não realiza distribuição.

9.7 Endereço da página da companhia securitizadora na rede mundial de computadores na qual podem ser encontrados os documentos exigidos pelo art. 46 da Resolução:

<https://fortesec.com.br/relacao-investidor/>