

FORMULÁRIO DE REFERÊNCIA DA FORTE SECURITIZADORA S.A.**Ano de Referência: 2025**

(Elaborado nos termos do Suplemento C da Resolução da Comissão de Valores Mobiliários nº 60, de 23 de dezembro de 2021)

3. Recursos humanos e tecnológicos**3.2. Descrever os recursos tecnológicos utilizados para controle das operações de securitização, incluindo os aspectos relacionados à segurança da informação e procedimentos de contingências.**

Além dos repositórios de dados na nuvem (descrito no item 9.3), os seguintes recursos tecnológicos são utilizados:

- Plataforma (Intranet) utilizada para disponibilizar documentos, relatórios e informações relativas aos processos e atividades organizacionais para o público interno (colaboradores).
- Plataforma (Extranet) utilizada para disponibilizar documentos, relatórios e informações relativos às operações / emissões geridas pela Securitizadora para o público externo (tomadores, investidores, agentes da operação, entre outros).
- *Software* de gestão de processos operacionais e organizacionais (BPM - *Business Process Management*), com módulo de *Business Intelligence* e análise integrado.
- *Software* de precificação de ativos, responsável pela gestão e cálculo dos ativos geridos pela Securitizadora, seus respectivos pagamentos e eventos no fluxo das operações.
- Sistema de informação de *Compliance*, utilizado para realizar pesquisas jurídicas, reputacionais e emissão de certidões.
- *Software* de gestão empresarial (ERP Financeiro) que contempla o armazenamento, processamento e gestão dos dados financeiros das operações.
- Suíte de aplicativos para escritório (Microsoft 365), utilizada para criação, leitura e armazenamento de arquivos das operações.

Aspectos adicionais relacionados à segurança da informação:

O acesso a dados de operações é baseado na regra *need to know*. Há, ainda, estrutura tecnológica para segregação de acessos e pastas específicas, em linha com as regras da Securitizadora relacionadas a Conflito de Interesses, Confidencialidade e Informações Privilegiadas.

Adicionalmente, a Securitizadora contrata serviço integrado de segurança e monitoramento de dados, baseado na detecção e prevenção de ameaças, e no gerenciamento da conformidade de todos os dispositivos do parque tecnológico. Esta solução gera relatórios e *dashboards* analíticos de todo o ecossistema.

Todo o parque tecnológico acessa uma rede interna restrita, separada da rede utilizada por visitantes e/ou terceiros e outros dispositivos, além de contar com a solução de antivírus e *antimalware*, sendo monitorados e atualizados de maneira centralizada e contínua.

Aspectos adicionais relacionados a procedimentos de contingências:

O plano de contingência da Securitizadora inclui armazenamento de todos os arquivos das operações na nuvem, com controle de versão e *backups* diários incrementais. Os *softwares* e banco de dados possuem *backup* diário, seguindo política padrão do respectivo fornecedor contratado.

Em relação aos *Softwares as a Service* (SaaS), as políticas de *backup* e retenção são de responsabilidade dos fornecedores contratados, além disso, os dados exportados são armazenados em nossa infraestrutura de nuvem, de acordo com a demanda diária e/ou mensal de cada área, mantendo o plano de contingência da Fortesec, descrito acima.

Adicionalmente, a política da Securitizadora referente a *backup* dos e-mails (*Microsoft Exchange*) é baseada em *snapshots* diários e possui uma retenção de arquivos e dados de 7 (sete) anos.