

FORMULÁRIO DE REFERÊNCIA
(competência 2023)

TI

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 (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 nosso fornecedor de nuvem.

Em relação aos *softwares as a service* (SaaS), as políticas de *backup* e retenção são de responsabilidade dos nossos fornecedores, 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 nosso plano de contingência 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.

8. Estrutura operacional e administrativa

8.1 Os departamentos técnicos (equipes) da Securitizadora são subordinados à Diretora de Novos Negócios, ao Diretor de Securitização ou ao Diretor de Compliance, conforme detalhado no item 8.2 abaixo, e possuem as seguintes atribuições:

Processos. A este departamento cabe:

- a) Analisar e definir métodos e processos da Securitizadora;
- b) Mapear o fluxo de atividades, identificando pontos a serem melhorados; e
- c) Propor melhoria contínua dos processos.

Tecnologia da Informação, Processos e Projetos. A este departamento cabe:

- a) Manter a infraestrutura tecnológica e o perfeito funcionamento dos hardwares, softwares, aplicações e acessos dos colaboradores da Securitizadora;
- b) Manter relacionamento com prestadores de serviço de tecnologia externos, garantindo a execução dos contratos e serviços exigindo o mais alto nível de qualidade;
- c) Garantir que a Securitizadora cumpra todos os requisitos operacionais de segregação de acessos;
- d) Providenciar estrutura interna de modo a garantir a comunicação com links de entidades do mercado organizado, notadamente o segmento CETIP da B3, conforme aplicável;
- e) Implantar e manter programa de treinamento de segurança da informação aos colaboradores da Securitizadora que tenham acesso a informações confidenciais, e a quem mais seja exigido por regulamentação vigente;
- f) Manter controles auditáveis e boas práticas de mercado em relação à governança, segurança da informação e prevenção à perda de dados, conforme Política de Segurança da Informação publicada; e,
- g) Diligenciar para o adequado funcionamento de estratégias tecnológicas em caso de contingência.

9. Regras, procedimentos e controles internos

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 no Manual de Compliance 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 apenas 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 no Manual de Compliance 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 (excluem-se os administradores de TI) 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 os administradores de TI (equipe de suporte interna e terceirizada) possui privilégios para alterar essa configuração.

As solicitações de inclusão, remoção e alteração de acesso dos usuários e grupos, além das alterações das permissões de acesso de quaisquer outros recursos gerenciados pela TI, são recebidas através do software de gestão de processo utilizado pela Securitizadora (item 3.2) com registro auditável das autorizações dos Gestores e/ou responsáveis pelos recursos.

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.

