SANTANDER TOTTA SEGUROS – COMPANHIA DE SEGUROS DE VIDA, S.A.

POLÍTICA DE CONTINUIDADE DE NEGÓCIO

INDICE

1 INTRODUÇÃO, ÂMBITO E OBJETIVOS

1.1 Introdução e âmbito

O presente documento estabelece a Política de Continuidade de Negócio e é aplicável à Santander Totta Seguros – Companhia de Seguros de Vida, S.A. doravante designada por "STS" ou "Sociedade".

O Sistema de Gestão de Continuidade de Negócio (doravante SGCN) é um processo de gestão holístico em que se identificam os acontecimentos potencias que podem resultar num maior impacto para a Sociedade, e se proporciona uma estrutura de atuação para garantir a sua resiliência e uma capacidade de resposta eficaz. Este sistema permite minimizar o impacto de uma eventual interrupção do funcionamento do negócio e proteger a reputação e imagem de marca, assim como, salvaguardar os interesses dos clientes e das demais principais partes interessadas da Sociedade. Deste modo, o presente documento foi aplicado no desenvolvimento e implementação do sistema de gestão de continuidade de negócio da Sociedade.

1.2 Objetivos

A Política de Continuidade de Negócio foi desenvolvida tendo em consideração as orientações do Grupo, os aspetos regulamentares e as especificidades do negócio da Sociedade. Assim, o sistema de Gestão de Continuidade do Negócio da Sociedade seguirá as orientações do Grupo que se encontram descritas nas Circulares do Banco Santander Totta, SA. Estas Circulares são de âmbito global em Portugal, aplicando-se às entidades do Grupo neste país.

Considerando ainda as especificidades da Companhia, a Política de Continuidade de Negócio define ainda os seguintes vectores a assegurar em caso de contingência:

2 INVESTIMENTOS

Os níveis de liquidez dos produtos em comercialização mais susceptíveis a resgates devem apresentar níveis adequados para acomodar um aumento de resgates em caso de contingência. Adicionalmente e por estrutura da carteira, uma percentagem expressiva dos activos subjacentes devem ser bastante líquidos com um objectivo de liquidação máxima a uma semana (no caso de fundos de investimento). O investimento em activos de classes não tradicionais (alternativos e *commodites*) só deverá ser executado através fundos que têm a classificação UCITS e que tenham liquidez diária. Como objectivo na classe obrigacionista não deve existir exposição material em *high-yield* ou dívida subordinada (a menos que em fundos que expressamente referenciem essas classes de activos), e as durações deverão ser genericamente curtas.

3 LIQUIDEZ

Os níveis de resgates nos produtos devem ser monitorizados diariamente, especialmente em momentos de elevada volatilidade e desvalorizações nos mercados financeiros. Deve ainda, em conjunto com a Sociedade Gestora de Activos (Santander Asset Management), ser adoptado um posicionamento em activos conservadores e de rápida venda em mercado em caso de contingência.

Caso se estime não existir nas carteiras de produtos, liquidez suficiente para fazer face ao volume expectável de resgates, deve ser incrementado o respectivo montante de liquidez para níveis que permitam dar a resposta adequada aos pedidos respectivos, considerando os prazos de liquidação necessários e a necessidade de assegurar o reembolso aos clientes.

4 OPERAÇÕES

A Política de Continuidade de Negócio da Companhia tem como objectivo assegurar o funcionamento integral dos seus serviços em cenário de contingência, prevendo para tal os processos necessários a assegurar a continuidade das operações, processos e trabalho de todos os colaboradores.

Assim, as ferramentas técnicas utilizadas pelos colaboradores devem ser capazes de ser reproduzidas em contexto de teletrabalho ou trabalho em instalações diferenciadas da companhia.

O apoio técnico da área de Tecnologia deve ser garantido a todo o tempo de forma a permitir assegurar a manutenção do funcionamento das ferramentas e resolução de quaisquer problemas que possam surgir com a deslocalização dos postos de trabalho.

A Companhia deve exigir dos seus fornecedores (sobretudo fornecedores críticos) a manutenção dos serviços e das respostas necessárias à garantia da operacionalidade da companhia em caso de cenários de contingência.

As equipas locais e corporativas do Grupo Santander devem fazer periodicamente testes de *hacking* às plataformas utilizadas para aferir os padrões de segurança da infraestrutura.

5 DESMATERIALIZAÇÃO

A Companhia deve ter o objectivo de desmaterializar por completo as suas operações, de forma a não depender de processos físicos que obriguem à presença obrigatória de colaboradores a todo o tempo nas instalações para que, em cenário de contingência, seja possível manter a operacionalidade da Companhia com o mínimo de impacto. Para tal, devem ser digitalizados todos os processos físicos existentes e que sejam base e material de trabalho dos colaboradores, devendo ser desincentivada a impressão para arquivo físico de documentação não original.

A Companhia deverá definir a utilização da assinatura electrónica em todos os processos e sempre que não seja necessário um original, incluindo em processos internos de autorização que se devem basear em processos electrónicos de *work-flow*, *email*, ou acessos partilhados a pastas.

Em contratos onde não seja necessária a assinatura qualificada (ou digital), deve ser promovida a assinatura electrónica sempre aposta pelos próprios, e deve ser considerada válida e com o pleno valor jurídico legal actualmente definido para esta tipologia de assinatura.

São admitidas reuniões não presenciais, seja por via telefónica, videoconferência ou outros meios telemáticos proporcionados por ferramentas autorizadas corporativamente, tendo as decisões tomadas nestes *fora* a mesma validade que as tomadas de forma presencial. Desta forma, em cenário de contingência, podem manter-se os compromissos agendados.

Devem ser privilegiadas as comunicações essenciais através dos canais electrónicos de forma a permitir manter as mesmas em cenário de contingência, devendo ser criados e normalizados os processos electrónicos.

Devem ser promovidos e privilegiados os contactos não presenciais, mas pessoais, com os clientes sempre que possível, seja por via telefónica, seja por via de correio electrónico ou ferramentas de comunicação alternativas (como sejam através de sites, sms, apps ou outros canais virtuais disponíveis), disponibilizando estes contactos nas comunicações oficiais e *site*, permitindo a manutenção das comunicações em cenário de contingência sem disrupções. As comunicações devem contudo sempre ser pessoais no sentido de serem assinadas pelos respectivos signatários de forma a serem identificáveis pelos clientes caso queiram responder.

6 COLABORADORES

Em caso de contingência, o teletrabalho ou trabalho remoto em instalações alternativas deve ser promovido, garantido e obrigatório em caso de se evidenciar ser mais seguro para o colaborador ou de permitir acrescentar protecção adicional, devendo ser minimizadas as idas e permanência nas instalações originais ao indispensável para assegurar processos críticos e /ou o serviço aos clientes.

Não deve depender de um único colaborador o acesso a determinada ferramenta, operativa ou processo, devendo ser determinados e definidos *back-ups* e múltiplos acessos de forma a permitir flexibilizar em cada momento a execução do trabalho.

Todos os colaboradores devem ter computadores portáteis ou soluções alternativas que permitam a deslocalização do posto de trabalho, ainda que com acrescentos técnicos adicionais para a circunstância eventual de trabalho remoto.

7 PREVISÃO EM CENÁRIOS DE *STRESS-TEST*

Devem ser considerados, para os exercícios anuais de *stress test*, cenários de contingência que possam impactar directamente a actividade da Companhia de forma a antecipar necessidades de ajustamento em termos de rácios de solvência, políticas de dividendos e outras estratégias financeiras de conservação da saúde financeira da Companhia.

8 CONTROLO DO DOCUMENTO

Responsabilidade

Departamento
Departamento de de Resseguro, de Solvência e Capital

Validação / Aprovação

Validação / Aprovação	Departamento	Data
Validação	Comité de Gestão de Riscos e Controlo Interno	22/06/2016
Aprovação	Conselho de Administração	30/06/2016
Validação	Direção de Risco Operacional	25/09/2017
Aprovação	Conselho de Administração	27/09/2017
Aprovação	Comissão Executiva por delegação outorgada pelo Conselho de Administração em 15/10/18	08/11/2018
Aprovação	Conselho de Administração	28/11/2019
Actualização	Conselho de Administração	20/04/2020

Histórico da versão

Versão	Data	Requisitante da alteração	Descrição da alteração
1.0	30/06/2016	Conselho de Administração	Versão Inicial
2.0	27/09/2017	Departamento de Gestão de Riscos, Atuarial e Controlo Interno	Revisão Anual 2017
3.0	08/11/2018	Departamento de Gestão de Riscos, Atuarial e Controlo Interno	Revisão Anual 2018
4.0	25/11/2019	Departamento de Resseguro, de Solvência e Capital	Revisão Anual 2019
5.0	20/04/2020	Departamento de Qualidade, Contencioso, Compliance e Operações de Vida Risco	Actualização 2020