1 Área responsável pelo assunto

1.1 Superintendência de Tecnologia.

2 Abrangência

2.1 Esta Política orienta o comportamento da BB Seguridade e suas sociedades controladas. Espera-se que as empresas coligadas definam seus direcionamentos a partir dessas orientações, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

3 Público-alvo

3.1 Esta Política alcança todos os membros de órgãos de governança, empregados e terceiros no exercício de suas atividades profissionais relacionadas à Companhia.

4 Regulamentação

4.1 Decreto nº 9.637, de 26 de dezembro de 2018.

5 Periodicidade de Revisão

5.1 Esta Política deve ser revisada a cada três anos ou, extraordinariamente, a qualquer tempo, e submetida ao Conselho de Administração para aprovação.

6 Sumário Executivo

6.1 Esta Política tem por objetivo estabelecer as diretrizes relacionadas à gestão de segurança da informação, nos termos da legislação e regulamentação aplicáveis.

7 Conceitos

7.1 Para fins desta Política são considerados os seguintes conceitos:

7.1.1 **Administrador de Acesso**: aquele que gerencia o direito de acesso às informações em meio eletrônico na dependência.

7.1.2 **Ativo**: são os bens e direitos que a empresa tem em um determinado momento.

7.1.3 **Ativo de Informação**: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas.

7.1.4 **Ciclo de vida da informação**: compreende as fases de vida da informação, que são: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte.

7.1.5 **Classificação da Informação**: identificar quais são os níveis de proteção que as informações demandam.

7.1.6 **Confidencialidade**: propriedade que garante que a informação está disponível ou revelada a usuário autorizado.

7.1.7 **Disponibilidade**: propriedade de ser acessível e utilizável por um usuário autorizado.

7.1.8 **Gestor da Informação**: área responsável pela gestão da informação (em suas diversas formas – impressa, escrita, em meio eletrônico, entre outros), durante todo o seu ciclo de vida, dentro do escopo de suas atribuições e/ou responsabilidades.

7.1.9 **Incidentes de Segurança da Informação**: qualquer ação que possa causar a quebra de confidencialidade, integridade e/ou disponibilidade das informações da Companhia.

7.1.10 **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

7.1.11 **Integridade**: salvaguarda da exatidão e completeza da informação e dos métodos de processamento de forma que as alterações sejam planejadas e autorizadas.

7.1.12 **Órgãos de Governança**: estruturas constituídas para promover o máximo alinhamento entre a gestão da Companhia (agentes) e os interesses dos sócios (principais): Assembleia Geral, Conselho de Administração, Conselho Fiscal, Comitê de Auditoria, Auditoria Independente, Auditoria Interna, Comitês Técnicos e Diretoria.

7.1.13 **Princípio de Segregação das Funções**: consiste na separação de atribuições ou responsabilidades entre diferentes pessoas, especialmente as funções ou atividades-chave de autorização, execução, aprovação, registro e revisão ou auditoria.

7.1.14 **Segurança da Informação**: preservação da confidencialidade, integridade e disponibilidade das informações.

7.1.15 **Terceiros**: pessoas físicas, que não são empregados da Companhia, e pessoas jurídicas, que estabeleçam relacionamento com a Companhia por interesse do serviço, previsão contratual ou imposição legal.

7.1.16 **Usuário**: aquele que tem acesso à informação corporativa.

8 Valores Associados

8.1 Confiabilidade, Respeito ao Cliente e Sentimento de Dono.

9 Diretrizes

9.1 Consideramos, na formulação desta Política, as diretrizes estabelecidas na Política de Segurança da Informação do nosso controlador, Banco do Brasil.

9.2 Tratamos a informação, na gestão empresarial, como ativo.

9.3 Planejamos, dimensionamos e orientamos a proteção dos ativos de informação para atender aos interesses estratégicos da Companhia.

9.4 Garantimos a confidencialidade, integridade e disponibilidade da informação em todo o seu ciclo de vida.

9.5 Protegemos e monitoramos os ativos de informação reduzindo a possibilidade de uma descontinuidade operacional em caso de incidentes de segurança da informação.

9.6 Classificamos a informação em relação ao seu valor ou criticidade para a Companhia.

9.7 Identificamos e corrigimos as vulnerabilidades, as ameaças, os riscos e os impactos nocivos que envolvam os ativos de informação da Companhia, por meio de procedimentos de teste e de avaliação periódicos, a intervalos regulares.

9.8 Aplicamos proteção aos ativos de informação de forma compatível com seu impacto aos resultados e reputação da Companhia, alcançando todos os processos, informatizados ou não.

9.9 Adotamos mecanismos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens e roubo, quando do tratamento (produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte) das informações geradas ou utilizadas pela Companhia.

9.10 Analisamos as ocorrências de subtração, violação ou divulgação indevida de informações, sob os aspectos legal e disciplinar, imputando responsabilização e, sob o aspecto técnico, corrigindo as vulnerabilidades.

9.11 Atribuímos a responsabilidade pela proteção das informações a pelo menos um gestor da informação.

9.12 Identificamos, nos sistemas de controle de acesso, cada usuário individualmente, responsabilizando-o, juntamente com o administrador que lhe concedeu o acesso, pelas atividades realizadas sob seu código de identificação.

9.13 Obedecemos ao princípio de segregação das funções de desenvolvimento de recursos, uso de recursos, administração da segurança e auditoria, na gestão da informação.

9.14 Disponibilizamos para os usuários as informações da BB Seguridade com o objetivo de viabilizar suas atividades profissionais na Companhia. Não permitimos a utilização das informações para qualquer atividade que viole esta Política.

9.15 Preservamos os mesmos quesitos de segurança adotados pela Companhia, na contratação de serviços ou de pessoas e no relacionamento com membros de órgãos de governança, empregados e terceiros.

9.16 Disseminamos questões sobre segurança da informação por meio de programas permanentes de conscientização, de abrangência geral, ou cursos de capacitação técnica para os usuários diretamente envolvidos na utilização de recursos.

9.17 Incentivamos as empresas nas quais temos participação a adotar os mesmos princípios e práticas na gestão da segurança da informação.

9.18 **Governança da Segurança da Informação das Sociedades Coligadas**

9.18.1 Reconhecemos que a exposição da Companhia aos riscos decorrentes da gestão da informação origina-se, também, da operação das sociedades coligadas.

9.18.2 Zelamos pelo interesse da Companhia orientando os representantes da BB Seguridade nos órgãos de governança das sociedades coligadas, sobre aspectos preventivos e detectivos relacionados à segurança da informação.

9.18.3 Promovemos intercâmbios técnicos entre as sociedades coligadas, a BB Seguridade e o Banco do Brasil.

9.18.4 Avaliamos indicadores e monitoramos os reportes aos órgãos de governança sobre as práticas de segurança da informação.

10 Data da Última aprovação pelo Conselho de Administração

10.1 27 de novembro de 2019.

11 Disposições Finais

11.1 Casos omissos nesta Política deverão ser encaminhados para deliberação do Conselho de Administração.

12 Tabela de Controle de Versionamento

12.1

Vigência	27.11.2019 a 27.11.2022
Versão	5
Histórico de Alterações	Alteração dos itens 1.1; 4.1; 5.1; 9.18.2 e 10.1