CCB 中国建设银行
China Construction Bank

GUIA DE MELHORES PRÁTICAS

CONGLOMERADO CCB BRASIL

CCB

GUIA DE MELHORES PRÁTICAS

CONGLOMERADO **CCB BRASIL**

CONFORMIDADE · AUTORREGULAÇÃO · PROTEÇÃO DE DADOS · GOVERNANÇA · CONTROLES INTERNOS · COMPLIANCE · CONFORMIDADE · PRIVACIDADE · COORPORATIVA · SEGURANÇA DA INFORMAÇÃO · PRIVACIDADE · ÉTICA · SEGURANÇA CIBERNÉTICA · GERENCIAMENTO DE RISCOS · PROTEÇÃO DE DADOS · ÉTICA · SEGURANÇA DA INFORMAÇÃO

Transparência e responsabilidade:
na prática, essa é a **PRÁTICA**.

Sumário

1 Breve mensagem da Diretoria

O Guia de Melhores Práticas do Conglomerado CCB Brasil é um documento elaborado sob as mais rigorosas normas de conduta e integridade, devendo pautar todo e qualquer relacionamento da Instituição, tanto interna quanto externamente.

Orientado e desenvolvido a partir dos valores descritos no Código de Ética e Conduta da Instituição, dos princípios técnicos determinados por seus gestores e de extensa legislação, deve ser observado igualmente por todos os níveis da Organização, sem distinção de hierarquia, bem como por todos que mantêm relacionamento com a Instituição.

É dever de cada colaborador repassar os conteúdos aqui apresentados a cada um dos fornecedores / prestadores de serviços, visando à redução de riscos para todos e proporcionando uma perfeita divisão das responsabilidades no cumprimento das leis.

Sua plena observância leva ao fortalecimento da imagem corporativa, ao incremento da noção de sustentabilidade e à perenidade do negócio. Integridade, transparência e respeito às normas são essenciais para o equilíbrio no ambiente de trabalho e no relacionamento com fornecedores / prestadores de serviço, além de incentivarem a criação de um círculo virtuoso de hábitos saudáveis com positiva repercussão dentro e fora do Conglomerado CCB Brasil.

Conselho Diretivo do Conglomerado CCB Brasil

2 Da importância deste documento

As diretrizes contidas neste Guia de Melhores Práticas têm o objetivo de orientar os stakeholders do Conglomerado CCB Brasil na proteção de seus ativos e na sensibilização para a prevenção, detecção e identificação de eventuais irregularidades. O conteúdo de Compliance aqui apresentado é baseado nas determinações legais e nas recomendações do Banco Central do Brasil e da Febraban, entre outras instituições, e tem seu devido respaldo e proteção legal.

É importante ressaltar seu papel consultivo como apoio estratégico na gestão dos recursos e na transmissão da cultura e dos valores contidos na missão e na visão do Conglomerado CCB Brasil. Ou seja, o Compliance ultrapassa a ideia fundamental de conformidade à regulamentação para atingir diversos aspectos da governança como um todo.

As sanções legais ou regulatórias decorrentes do mau uso ou do descumprimento das disposições e normas deste guia, como riscos de imagem, danos à reputação ou perda financeira, são consideradas irreparáveis ao patrimônio tanto material quanto imaterial da Instituição. Portanto, todos os colaboradores, independentemente do cargo que ocupem, assim como aqueles que mantêm relacionamento com a Instituição, têm responsabilidade por seu integral e efetivo cumprimento.

3 Como usar este guia

Deste documento constam as mais importantes resoluções normativas publicadas para assegurar condutas empresariais responsáveis em todos os níveis de relacionamento no Conglomerado CCB Brasil. Elas são essenciais para o pleno cumprimento das regulamentações internas e externas, evitando-se, assim, o risco de medidas administrativas punitivas e de sanções legais ou regulatórias. Além disso, o correto uso deste guia gera segurança no desempenho e crescimento do valor estratégico, resguardando a Instituição de perdas reputacionais ou financeiras.

Para efeito de facilitação do acesso aos volumes originais das normas, as fontes estão indicadas ao final de cada um dos capítulos para um eventual aprofundamento nos temas aqui tratados. Os principais links dos documentos estão disponíveis ao final dos seis capítulos deste Guia de Melhores Práticas do Conglomerado CCB Brasil.

Cabe ressaltar ainda que, além da leitura completa deste documento, é fundamental, para a ampla percepção dos valores éticos que fundam o Conglomerado CCB Brasil, que todos os colaboradores disseminem a cultura da conformidade em todos os contextos da Instituição, inclusive para o público externo. Caso haja alguma dúvida com relação aos termos utilizados, há um glossário ao final para que nenhuma informação escape ao leitor.

4 Das legislações aplicáveis

Veja a seguir, de forma didática e condensada em sete conjuntos de temas, as linhas gerais das normas e legislações correntes aplicáveis nas respectivas disposições internas do Conglomerado CCB Brasil. **Leia com atenção.**

4.1

Compliance no Conglomerado CCB BRASIL

Sobre as políticas de compliance, governança corporativa e controles internos.

O QUE É O COMPLIANCE?

O termo compliance vem do inglês “to comply” e quer dizer “estar em conformidade”. É o princípio número um da governança corporativa e visa a neutralizar os chamados riscos de conformidade, ou seja, aqueles decorrentes do descumprimento de leis, normas, diretrizes (nacionais ou estrangeiras) ou compromissos assumidos em códigos de autorregulação.

O Conselho de Administração do CCB Brasil é quem estabelece a estrutura interna de Compliance, sua implementação e manutenção, além de definir suas diretrizes e estabelecer suas práticas para mitigação dos riscos.

A Governança de Conformidade deve envolver o Conselho de Administração, o(a) Chief Executive Officer (CEO), o(a) Chief Risk Officer (CRO), o(a) Chief Compliance Officer (CCO) e a Diretoria Executiva de Riscos e Compliance, cabendo a todos os colaboradores do Conglomerado CCB Brasil e aqueles que mantém relacionamento com a instituição a responsabilidade por seu integral e efetivo cumprimento.

PARA QUE SERVE O COMPLIANCE?

Para além do natural cumprimento das leis, o Compliance serve basicamente para disseminar e instalar, em todas as áreas da Instituição, a cultura da conformidade. Desse modo, resulta em um exemplo de conduta para todos os colaboradores e outros com quem a Instituição mantenha relacionamento, especialmente da alta administração, que deve respaldá-lo e estabelecer suas diretrizes. Diversos outros benefícios decorrem a partir daí, por exemplo:

VALORIZAÇÃO da conscientização de todos os públicos de relacionamento, incluindo colaboradores, clientes, parceiros, fornecedores/prestadores de serviços, governos e a sociedade sobre a importância das diretrizes dessa política;

PROMOÇÃO da redução de riscos em todos os níveis do negócio, desde o operacional até o estratégico;

APROXIMAÇÃO com órgãos reguladores, fiscalizadores, associações de classe, bem como auditores independentes e externos;

CORREÇÃO constante dos itens relacionados à não conformidade com o pronto atendimento e observância das leis;

ASSISTÊNCIA à Diretoria Executiva de Riscos e Compliance e a toda a estrutura de conformidade em suas atribuições relacionadas à informação e disseminação da cultura da conformidade;

AUXÍLIO às áreas de negócios no conhecimento e na observância dos normativos emitidos pelos órgãos reguladores externos e normativos internos, apontando o seu impacto.

COMO O COMPLIANCE SE APLICA NO CONGLOMERADO CCB BRASIL?

A Política de Conformidade formaliza as diretrizes do Conselho de Administração do Conglomerado CCB Brasil e estabelece a estrutura interna de Compliance, sua implementação e manutenção. Sua finalidade é buscar a aderência das medidas voltadas à realização dos objetivos institucionais às leis e regulamentos internos e externos, bem como proporcionar o alcance de tais objetivos de forma eficaz.

No desempenho de suas funções, o Compliance avalia as regulamentações recebidas, divulga-as para as divisões possivelmente impactadas, realiza testes de aderência às legislações, autorregulações e normativos internos, de acordo com a metodologia estabelecida, e, quando necessário, acompanha os planos de ação e cronogramas para o saneamento de gaps.

Para o pleno funcionamento do Compliance, o Conglomerado CCB Brasil deve prever a alocação de pessoal em número suficiente, adequadamente treinado e com experiência necessária para o exercício das atividades relacionadas à função de fiscalização da conformidade. Assim, o Conselho de Administração trabalha:

ASSEGURANDO a gestão, a efetividade, a comunicação e a continuidade das políticas de conformidade;

CERTIFICANDO-SE de que medidas corretivas ocorrerão prontamente para a correção das falhas identificadas;

MONITORANDO continuamente o ambiente regulatório e divulgando os normativos aplicáveis para a atuação das áreas responsáveis, ou seja, realizando a gestão do conjunto de normativos internos e prestando informações aos colaboradores e todos que se relacionam com a Instituição através de ampla divulgação;

AVALIANDO a aderência da Instituição às regulamentações e acompanhando as alterações nos manuais de processos e outras políticas institucionais que digam respeito à conformidade nas atividades;

ELABORANDO um relatório, com periodicidade mínima anual, contendo o sumário dos resultados das atividades relacionadas à função de conformidade, com suas principais conclusões, recomendações e providências necessárias, e submetendo esse relatório à Diretoria Executiva de Riscos e Compliance, ao Comitê de Compliance; ao Comitê de Auditoria Interna; e ao Comitê de Diretoria Executiva;

COMUNICANDO de maneira sistemática e oportuna ao Conselho de Administração os resultados das atividades relativas à conformidade;

ATUANDO de forma independente e autônoma, com livre acesso às informações necessárias para o exercício de suas atribuições.

QUAIS SÃO OS EFEITOS DO COMPLIANCE?

O cumprimento das regulamentações vigentes, bem como das diretrizes de conformidade previstas em política específica e nos demais normativos internos do Conglomerado CCB Brasil, produz um efeito perene de credibilidade e transparência essencial para o desenvolvimento dos negócios, e sendo monitorado e fiscalizado de acordo com o Relatório de Compliance, emitido periodicamente.

O descumprimento de compliance pode levar a sérias medidas administrativas punitivas, sanções legais ou regulatórias ou ainda resultar em significativas perdas reputacionais ou financeiras.

A Lei n° 13.506, de 13 de novembro de 2017, que estabelece o processo administrativo sancionador na esfera de atuação do Banco Central do Brasil e da Comissão de Valores Mobiliários, define como INFRAÇÕES:

REALIZAR operações no Sistema Financeiro Nacional, no Sistema de Consórcios e no Sistema de Pagamentos Brasileiro não autorizadas, vedadas ou em desacordo

com a autorização concedida, com princípios previstos em normas legais e regulamentares que regem a atividade autorizada pelo Banco Central do Brasil;

OPOR embaraço à fiscalização do Banco Central do Brasil;

DEIXAR de fornecer ao Banco Central do Brasil documentos, dados ou informações cuja remessa seja imposta por normas legais ou regulamentares;

FORNECER ao Banco Central do Brasil documentos, dados ou informações incorretos ou em desacordo com os prazos e as condições estabelecidos em normas legais ou regulamentares;

ATUAR como administrador do contrato social das instituições financeiras, das instituições supervisionadas pelo Banco Central do Brasil e dos integrantes do Sistema de Pagamentos Brasileiro (caput do art. 2º dessa Lei) sem a prévia aprovação pelo Banco Central do Brasil;

DEIXAR de adotar controles internos destinados a conservar o sigilo de que trata a Lei Complementar nº 105, de 10 de janeiro de 2001;

NEGOCIAR títulos, instrumentos financeiros e outros ativos, ou realizar operações de crédito ou de arrendamento mercantil, a preços destoantes dos praticados pelo mercado, em prejuízo próprio ou de terceiros;

SIMULAR ou estruturar operações sem fundamentação econômica, com o objetivo de propiciar ou obter, para si ou para terceiros, vantagem indevida;

DESVIAR recursos de pessoa mencionada no caput do art. 2º dessa Lei ou de terceiros;

INSERIR ou manter registros ou informações falsos ou incorretos em demonstrações contábeis ou financeiras ou em relatórios de auditoria de pessoa mencionada no caput do art. 2º desta Lei;

DISTRIBUIR dividendos, pagar juros sobre capital próprio ou, de qualquer outra forma, remunerar os acionistas, os administradores ou os membros de órgãos previstos no estatuto ou no contrato social de pessoa mencionada no caput do art. 2º dessa Lei com base em resultados apurados a partir de demonstrações contábeis ou financeiras falsas ou incorretas;

DEIXAR de atuar com diligência e prudência na condução dos interesses de pessoa mencionada no caput do art. 2º dessa Lei; deixar de segregar as atividades de pessoa mencionada no caput do art. 2º dessa Lei daquelas de outras sociedades, controladas e coligadas, de modo a gerar ou contribuir para gerar confusão patrimonial; ou deixar de fiscalizar os atos dos órgãos de administração de pessoa mencionada no caput do art. 2º dessa Lei, quando obrigado a isso;

DESCUMPRIR normas legais e regulamentares do Sistema Financeiro Nacional, do Sistema de Consórcios e do Sistema de Pagamentos Brasileiro, determinações do Banco Central do Brasil, bem como seus respectivos prazos, adotadas com base em sua competência;

Quanto ao cálculo das penas aplicáveis no âmbito administrativo, em caso de infrações, a Resolução BCB nº 131 do Banco Central do Brasil dispõe sobre os diversos parâmetros a serem considerados. Estes variam desde a capacidade econômica do infrator até a reprovabilidade e a duração da conduta irregular, passando, é claro, pelo montante das operações e o grau de lesão ou perigo decorrente dos delitos.

Na dosimetria das penalidades, multa, inabilitação temporária, cassação ou advertência, há gradações conforme o tipo de infração, instituição ou atividade envolvidas. Alguns agravantes e atenuantes, tais como reincidência em prazo inferior a três anos ou dolo, também estão indicados na norma. Além disso, a lei determina os valores de multas combinatórias fixadas conforme o tipo e o porte das instituições autorizadas pelo BACEN.

Reforçamos que, no Conglomerado CCB Brasil, todos os eventuais casos de descumprimento estão sujeitos, sem prejuízo das responsabilidades do Comitê de Ética, às infrações, penalidades, medidas coercitivas e meios alternativos de solução de controvérsias aplicáveis às instituições financeiras, às demais instituições supervisionadas pelo Banco Central do Brasil e aos integrantes do Sistema de Pagamentos Brasileiro.

REFERÊNCIAS DESTE CONTEÚDO

Lei nº 13.506, de 13 de novembro de 2017; Resolução CMN nº 4.557, de 23 de fevereiro de 2017; Resolução CMN nº 4.595, de 28 de agosto de 2017; Resolução BCB nº 131 de 20 de agosto de 2021; Resolução CMN nº 4.968, de 25 de novembro de 2021.

4.2

Programa de Privacidade e Proteção de Dados no Conglomerado CCB BRASIL

Sobre a responsabilidade no tratamento das informações confidenciais.

O QUE É PRIVACIDADE E PROTEÇÃO DE DADOS?

A privacidade está prevista no rol de garantias e direitos fundamentais, definidos como invioláveis constitucionalmente. A privacidade é um conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições. Legalmente, a privacidade de dados pessoais é definida pela LGPD, Lei Geral de Proteção de Dados Pessoais, composta de 65 artigos e em vigor no Brasil desde 2020. Trata-se de uma ferramenta que visa à proteção dos danos causados pela ruptura desses direitos ou da utilização sem consentimento dos dados dos usuários.

O Programa de Privacidade e Proteção de Dados é uma diretriz obrigatória para todas as empresas do Conglomerado CCB. Seu cumprimento integral e efetivo cabe aos administradores, colaboradores, estagiários e fornecedores/prestadores de serviços que apoiam a operação, a sustentação e/ou o armazenamento de suas informações, utilizando-se ou não das instalações físicas e infraestrutura tecnológica da Instituição.

Assim, websites, sistemas, documentos físicos ou digitais, e serviços baseados em nuvem, hospedados dentro ou fora do Conglomerado CCB Brasil, estão sujeitos ao controle da Instituição em todos os ambientes, seja por meios eletrônicos ou manuais, reais ou virtuais.

PARA QUE SERVE O PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS?

O framework de Privacidade e Proteção de Dados estabelece diretrizes, orientações, responsabilidades e boas práticas para a concepção de efetiva proteção de dados na Instituição. Para mitigar eventuais riscos de incidentes relacionados ao tratamento de dados pessoais, o Conglomerado CCB Brasil atua de modo a:

PROTEGER o direito e a liberdade de pessoas físicas, garantindo o sigilo de seus dados pessoais e que estes sejam tratados com a máxima seriedade, exigindo dos fornecedores/prestadores de serviços o mesmo zelo, discrição e prudência quanto à proteção e à privacidade das informações;

TRATAR somente daqueles dados pessoais necessários para o cumprimento de suas atividades diárias, inclusive dados pessoais de colaboradores, contatos de fornecedores / prestadores de serviços e parceiros comerciais, entre outros;

COMPREENDER que os dados pessoais formam o ativo mais precioso da Organização, e por isso, adotar perenemente medidas pertinentes visando à proteção total dessas informações;

PREZAR tanto pela privacidade quanto pela segurança das informações de clientes, colaboradores, visitantes e websites, tratando-os com o devido zelo e sempre de acordo com o Código de Ética e Conduta do Conglomerado CCB Brasil e a Lei Geral de Proteção de Dados;

GARANTIR que informações e dados pessoais sejam acessados apenas por pessoal devidamente autorizado e qualificado, e em nenhuma circunstância ceder, vender ou compartilhar tais informações e dados com terceiros sem a devida

autorização sempre para procedimentos específicos, inclusive por decisão judicial, reservando ao Conglomerado CCB Brasil a prerrogativa de destruí-los após o devido uso;

FAVORECER a leitura, a compreensão, o cumprimento e a disseminação das políticas de proteção de dados do Conglomerado CCB Brasil a fornecedores / prestadores de serviços, parceiros comerciais e quaisquer terceiros que trabalhem direta ou indiretamente com a Instituição.

COMO O PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS SE APLICA NO CONGLOMERADO CCB BRASIL?

Com a criação do Comitê de Privacidade e Proteção de Dados (CPPD) e do Grupo de Trabalho de Privacidade e Proteção de Dados (GTPPD), foram instituídos dois âmbitos específicos para o tratamento de assuntos relativos à privacidade e proteção de dados no Conglomerado CCB Brasil. O Grupo reporta-se ao Comitê e este ao Data Protection Officer (DPO) cuja nomeação e dados são divulgados publicamente. Os gestores responsáveis pelos departamentos e seus respectivos processos devem agir da seguinte forma:

RESPEITANDO os princípios da transparência e das boas práticas, ou seja, observando a privacidade dos titulares quanto à finalidade, à necessidade, à retenção de dados e sua devida minimização/criptografia/anonimização para proteção da identidade do titular dos dados no caso de um incidente de dados pessoais;

TOMANDO as medidas necessárias para tratamento dos dados com a melhor qualidade possível, buscando sempre exatidão, clareza e relevância na atualização dos dados para suas respectivas finalidades;

MANTENDO o registro do tratamento de dados de acordo com suas respectivas finalidades a fim de que seja possível garantir a transparência com os titulares dos dados pessoais;

UTILIZANDO medidas técnicas e administrativas de segurança aplicáveis de acordo com os procedimentos internos preestabelecidos, bem como adotando medidas preventivas para mitigar riscos de danos e incidentes em virtude de tratamento ilegal ou não autorizado;

ABSTENDO-SE de tratar dados pessoais com fins discriminatórios ilícitos ou abusivos;

SEGUINDO as orientações contidas no guia específico sobre o tema e seus procedimentos para registro de cada nova atividade no tratamento de dados pessoais;

COMUNICANDO sempre o tratamento dos dados e informando, por meio de aviso de privacidade, quem é o agente de tratamento responsável pelo tratamento dos dados, quais as finalidades para tanto, seus locais de destinação, se existe o uso compartilhado de dados e com quais terceiros e, principalmente, sobre os direitos e como exercê-los;

TOMANDO medidas adequadas para garantir a máxima transparência nas ocasiões excepcionais em que não seja possível emitir o aviso de privacidade, por exemplo, quando não houver relação entre o agente de tratamento e o titular;

CONSULTANDO o guia específico sobre o tema da gestão de consentimento de tratamento conforme cada situação legal permitida, como em casos de proteção de crédito, execução de contrato, cumprimento de uma ação legal, uso compartilhado de dados e tutela da saúde, entre outras hipóteses;

CONSIDERANDO com atenção os chamados dados pessoais sensíveis e só autorizando o seu tratamento quando for indispensável nas seguintes hipóteses: cumprimento de obrigação legal ou regulatória; exercício regular de direito (processos judiciais, administrativos ou arbitrais); consentimento do titular de forma específica e

destacada para finalidades específicas; tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou prevenção a fraude e segurança do titular em processos de identificação e autenticação de cadastro em sistemas eletrônicos (situações de coleta de biometria para acesso a locais físicos restritos, efetivação ou confirmação de transações bancárias, entre outras), sempre assegurando que o tratamento não se sobreponha a direitos e liberdades fundamentais do titular;

CUIDANDO para que dados pessoais que eventualmente revelem dados sensíveis — por exemplo, na análise de consumo de produto ou serviço — não exponham nem sugiram a identificação do cliente, seja pelo tipo de local de compra ou pela preferência política, religiosa, sexual, etc. Nesses casos, os dados comuns devem ser tratados como sensíveis;

RESERVANDO aos dados de crianças e adolescentes um tratamento de ainda maior proteção em relação a outros dados pessoais. Esses dados não costumam ser tratados pelo Conglomerado CCB Brasil, considerando que os produtos e serviços ofertados pelo Conglomerado não têm como foco esse público. Em casos excepcionais, tais dados poderão ser tratados, sendo obrigatório obter o consentimento específico dos pais ou responsáveis legais do titular, salvo em casos nos quais o tratamento for base legal para defesa em processos judiciais, administrativos ou arbitrais;

PROPORCIONANDO amplo direito de acesso dos titulares a seus dados pessoais. As respostas para tais solicitações serão dadas de forma simplificada e completa, de acordo com o previsto em lei, dentro de um prazo de 15 (quinze) dias a contar do requerimento do titular, resguardados os segredos comerciais e industriais. Além disso, os titulares possuem amplos direitos de retificação, cancelamento, esquecimento, bloqueio, oposição, portabilidade ou anonimização de seus dados quando processados em excesso ou de forma ilegal. O titular também terá direito a solicitar a eliminação de seus dados pessoais quando a base legal para o tratamento for proveniente de consentimento, salvo nas hipóteses de retenção previstas em lei. O titular também poderá solicitar a portabilidade de seus dados pessoais a outro prestador de serviços ou produtos mediante solicitação expressa, de acordo com a regulamentação da Autoridade Nacional de Proteção de Dados (ANPD) e órgãos reguladores, resguardados os segredos comerciais e industriais;

PERMITINDO a transferência internacional de dados pessoais nos casos em que haja o mesmo nível de proteção adequado à Lei Geral de Proteção de Dados (LGPD) no país destino, com consulta prévia ao CPPD. Toda transferência internacional

de dados, bem como qualquer outro tratamento de dados pessoais, deve ser registrada e submetida a processo de nova atividade de tratamento determinado pela diretriz de comunicação. Ainda assim, somente será permitida a transferência internacional de dados desde que:

- **o controlador** ofereça e garanta o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de cláusulas contratuais ou normas corporativas globais;
- **o titular** tenha fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo-o claramente de outras finalidades, conforme as diretrizes de gestão de consentimento nessa política;
- **a ANPD** autorize a transferência internacional;
- **a transferência** seja necessária para proteger os interesses vitais do titular dos dados ou de outras pessoas (terceiros), caso o titular dos dados seja física ou legalmente incapaz de dar consentimento;
- **a transferência** resulte de compromisso assumido em acordo de cooperação internacional;

GARANTINDO que os dados pessoais em posse do CCB Brasil não sejam fornecidos a terceiros não autorizados, incluindo familiares ou amigos de seus colaboradores, entidades privadas e órgãos governamentais, sem que haja autorização da Companhia, demanda oriunda de órgão regulador ou ordem judicial para tanto;

REPORTANDO ao CPPD sempre que colaboradores forem solicitados a divulgar dados pessoais a terceiros, inclusive em caso de demanda de órgão regulador ou ordem judicial. Será obrigatória a participação dos colaboradores em treinamento específico que lhes permita lidar efetivamente com esse risco. Todas as solicitações de fornecimento de dados devem ainda ser respaldadas por ampla documentação e devidamente armazenadas junto com a autorização do CPPD;

OBRIGANDO colaboradores, parceiros e terceiros a notificar o CCB Brasil em caso de quaisquer alterações no tratamento de dados pessoais para permitir a atualização imediata dos registros, conforme guia específico do tema. É de responsabilidade

PROGRAMA DE PPD

do CCB Brasil garantir que qualquer notificação sobre mudança de circunstâncias seja registrada, recebida e devidamente encaminhada ao GTPPD;

RETIFICANDO dados pessoais imprecisos ou desatualizados que tenham sido compartilhados com a Companhia e informando, quando detectada, a defasagem nos registros a outros departamentos e terceiros;

FAZENDO o devido mapeamento de controle de dados pessoais e desenvolvendo relatórios de acordo com as normas de privacidade do guia específico sobre o tema;

AVALIANDO tecnicamente os riscos relacionados ao impacto do tratamento de dados da Companhia, considerando e analisando as deliberações do Departamento Jurídico e de Compliance e as técnicas apresentadas no Relatório de Impacto à Proteção de Dados (RIPD), conforme descrito no guia específico para riscos, que apresenta medidas de segurança, técnicas ou administrativas, de acordo com seu grau de risco e respectiva priorização;

CONCEBENDO e CONSIDERANDO a privacidade e proteção de dados em todas as etapas, desde a criação até a implementação de novos produtos, processos, procedimentos e sistemas;

ESTENDENDO esse padrão como um projeto de monitoramento de novos recursos e garantindo que a privacidade e proteção de dados seja cumprida no decorrer de todas as atividades criadas;

REPORTANDO imediatamente ao GTPPD eventuais suspeitas de violações e incidentes relacionados ao tratamento de dados pessoais realizados pelo CCB Brasil ou por terceiros em seu nome, sempre seguindo os canais de comunicação interna e as diretrizes de Gerenciamento de Incidentes. O GTPPD analisará a necessidade de comunicação ao Grupo de Respostas a Incidentes, de acordo com a criticidade e complexidade da ocorrência e as diretrizes estabelecidas na Política de Resposta a Incidentes, parte integrante da documentação do conglomerado CCB Brasil. A identificação de riscos pelo não cumprimento deverá ser reportada ao CPPD de forma imediata para que seja solicitada uma auditoria independente;

ARMAZENANDO pelo prazo legal toda a documentação relacionada às suspeitas com o objetivo de registrar e acompanhar internamente eventuais incidentes de segurança e, em caso de dúvidas urgentes, contatando diretamente um dos membros do GTPPD;

APOIANDO a Política de Resposta a Incidentes de privacidade e tomando todas as medidas possíveis de maneira a minimizar os impactos causados, visando a recuperar a integridade e a confidencialidade dos dados pessoais. Para isso,

devem ser elaborados, realizados e monitorados planos de ação relacionados ao controle da privacidade;

REALIZANDO auditorias periódicas com a finalidade de garantir o cumprimento dessas e de outras políticas relacionadas à privacidade e à proteção de dados;

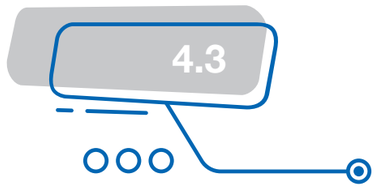
DISPONIBILIZANDO a todos os colaboradores ferramentas de procedimentos e controles internos, sistemas, medidas preventivas e atividades dos departamentos com o objetivo de manter a Companhia em conformidade com as normas e na observância dos regulamentos relacionados à privacidade e à proteção de dados pessoais.

QUAIS SÃO OS EFEITOS DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS?

A aplicação de todas as recomendações no tratamento de dados tem como efeito prático a prevenção, a redução e a mitigação das perdas decorrentes de incidentes de segurança da informação ou de ruptura de contratos de privacidade. Tais ocorrências não admitem descuidos, pois afetariam diretamente os ativos de informação do Conglomerado CCB Brasil. Ao evitá-las, reforça-se a confiança estabelecida entre as partes interessadas, eliminam-se danos à reputação e amplia-se a percepção positiva da Instituição.

REFERÊNCIAS DESTE CONTEÚDO

Lei n° 13.709/2018 — Lei Geral de Proteção de Dados (LGPD).



Segurança da Informação no Conglomerado CCB BRASIL

Sobre as diretrizes das políticas de segurança dos ativos de informação.

O QUE É SEGURANÇA DA INFORMAÇÃO?

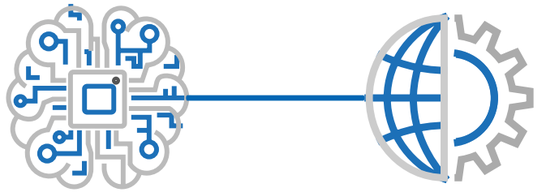
A Segurança da Informação (SI) é um grande sistema de proteção de um vasto conjunto de ativos de informação. Apesar de estar diretamente ligado à cibernética e ao armazenamento de dados, possui uma estrutura ainda mais ampla do que um complexo computacional, envolvendo premissas e valores como a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade.

O Conglomerado CCB Brasil é responsável pela definição e aplicação das políticas internas envolvendo a Segurança da Informação, bem como do suporte a todos os ativos a ela relacionados. O cumprimento dessas normas, a responsabilidade por sua constante manutenção e o suporte contínuo para a segurança são inerentes às funções e às tarefas diárias de todos os colaboradores, terceiros e fornecedores/ prestadores de serviços, interna e externamente.

PARA QUE SERVE A SEGURANÇA DA INFORMAÇÃO?

A Segurança da Informação no Conglomerado CCB Brasil tem como função assegurar, com responsabilidade, a confidencialidade, a disponibilidade e a integridade das informações confiadas pelas partes interessadas, incluindo, além dos clientes, também os colaboradores, investidores, terceiros e outros parceiros de negócios.

As políticas de SI são aplicáveis a todos os profissionais que utilizam os recursos de informática e dados do Conglomerado CCB Brasil e garantem o pleno funcionamento de todo o sistema operacional da Instituição, possibilitando desde a auditoria da conformidade com os contratos até a verificação do nível de controle do ambiente em que se inserem o sistema de informações e a proteção de dados pessoais.



COMO SE APLICA A SEGURANÇA DA INFORMAÇÃO NO CONGLOMERADO CCB BRASIL?

A Segurança da Informação no Conglomerado CCB Brasil estabelece controles para que nenhum terceiro, fornecedor/ prestador de serviço possa acessar dados pessoais mantidos pelo Conglomerado sem a celebração de contrato de confidencialidade de dados. Essas diretrizes devem ser aplicadas a todos os ambientes, sistemas, pessoas e processos pela Divisão de Segurança da Informação, responsável pela Gestão de Segurança da Informação no Conglomerado CCB Brasil, que deverá promover ações.

ASSEGURANDO que o Conglomerado CCB Brasil esteja preparado de forma a se prevenir contra diferentes tipos de fraudes; estabelecendo mecanismos para a proteção do sigilo das informações sob sua custódia; promovendo a segregação das funções de operacionalização, controles e liquidação de forma a evitar eventuais fraudes ou erros operacionais, bem como não permitindo a utilização de informações privilegiadas em benefício próprio ou de terceiros;

GARANTINDO o cumprimento de leis e normas que regulamentam as atividades do Conglomerado CCB Brasil de forma a obter aderência à legislação e regulamentações aplicáveis;

PREVENINDO a ocorrência de problemas ou dificuldades que afetem a segurança das informações sob posse ou responsabilidade dos usuários e zelando pela segurança das informações geradas ou administradas pela Empresa e utilizadas em quaisquer âmbitos de relacionamento, sejam eles profissionais ou pessoais, obedecendo aos requisitos contratuais e legais e às normas da organização;

AVALIANDO os requisitos legais aplicáveis às informações sob a responsabilidade do usuário, bem como a relação dessas normas com os controles internos e externos, visando à promoção de sua aderência;

ADMINISTRANDO de forma segura ambientes, informações, ativos de sistemas de informação e mídias que contenham quaisquer informações pertencentes ao Conglomerado CCB Brasil ou por ele custodiadas;

CONHECENDO o sistema de Segurança da Informação, com o intuito de evitar a ação de quaisquer tipos de fraudadores ou deles ser vítima;

GUARDANDO rigoroso sigilo sobre toda e qualquer informação, principalmente privilegiada, sendo-lhe vedado valer-se da informação para obter vantagem para si ou para outrem;

SUGERINDO mudanças em processos de modo a trazer maior proteção às informações do Conglomerado CCB Brasil e denunciar práticas que estejam em desacordo com as Políticas de Segurança da Informação do Conglomerado, assim como as que estejam em desacordo com o Código de Ética e Conduta ou com as leis em vigor;

CUMPRINDO integralmente as normas que compõem as Políticas de Segurança da Informação do Conglomerado CCB Brasil e zelando para que sejam sempre respeitadas, inclusive comunicando à Empresa situações irregulares ou suspeitas;

ASSEGURANDO que os usuários estejam cientes de ameaças que possam afetar negativamente a segurança das informações e se ocupem em orientar e apoiar esta política por meio da disseminação da cultura de segurança. A Divisão de Segurança da Informação deverá providenciar treinamento e conscientização geral sobre o tema para que todos os colaboradores e todos que mantêm relacionamento com o Conglomerado CCB Brasil possam implementar e disseminar suas bases de acordo com a necessidade e o conteúdo específico das respectivas áreas;

CUIDANDO para que todas as providências sejam tomadas de forma a evitar quaisquer ações ou situações que possam expor o Conglomerado CCB Brasil a perdas financeiras, materiais ou humanas, direta ou indiretamente, potenciais ou reais, e assim comprometer seu negócio;

PROTEGENDO a informação corporativa contra a divulgação, modificação, exclusão, destruição e acesso por pessoas não autorizadas e jamais colocando as informações do Conglomerado CCB Brasil ou os processos de informação em qualquer situação de risco. Todo colaborador e todos que mantêm relacionamento com o Conglomerado CCB Brasil devem assinar um termo em que declara seu conhecimento e total aderência às normas e procedimentos das Políticas de Segurança da Informação do Conglomerado CCB Brasil e de seu Código de Ética e Conduta, antes que lhe seja concedido acesso a qualquer tipo de informação;

PRESERVANDO e armazenando por tempo determinado pela Empresa ou por legislação vigente as informações do Conglomerado CCB Brasil, com acesso somente através de recursos devidamente autorizados pelo Conglomerado;

DEFENDENDO e protegendo de acesso externo as contas de usuário e suas senhas;

INVESTIGANDO prontamente qualquer possível causa de problemas, incidentes ou riscos de segurança e aplicando todas as medidas necessárias para impedir ou minimizar os danos;

ATENTANDO para que as estações de trabalho sejam monitoradas, equipadas e programadas com login e senha para acesso (logon), com bloqueio de tela e devida solicitação de senha para reinício, bem como encerramento automático quando ocioso;

MAPEANDO os processos mais críticos dos riscos e identificando, juntamente com o responsável pelo processo, as ações de segurança específicas a serem aplicadas com o objetivo de reforçar a segurança e garantir a exatidão das atividades de controle e prevenção de riscos nas operações de negócio e infraestrutura;

MANTENDO uma equipe competente e preparada para dar andamento ágil ao Processo de Gestão de Riscos, combatendo com eficiência a ocorrência de casos de fraudes nos ambientes do Conglomerado CCB Brasil;

CONTROLANDO a transferência eletrônica ou física de informações entre o Conglomerado CCB Brasil, terceiros e fornecedores/prestadores de serviço de maneira planejada a fim de assegurar a proteção e o armazenamento adequado. Esses terceiros, por receberem a informação do Conglomerado CCB Brasil, deverão demonstrar que dispõem de políticas e práticas para assegurar disponibilidade, integridade e confidencialidade, além de capacidade de recuperação dos ativos de informação, de forma a atender ou exceder as políticas e práticas internas do Conglomerado CCB Brasil. Um acordo por escrito que contenha cláusulas de proteção da informação em trânsito contra perda, divulgação e dano, aplicáveis de acordo com a classificação da informação e natureza do relacionamento comercial, deve ser firmado como garantia de segurança;

ESTABELECENDO processos e procedimentos para responder às violações de segurança, eventos e incidentes anormais ou suspeitos, com o objetivo de minimizar os danos aos ativos de informação, e permitindo a identificação e punição de seus autores, em acordo com a Política de Resposta a Incidentes. Tais processos deverão ser baseados na dimensão do risco e formalmente documentados. Essa documentação deve conter instruções detalhadas e devidamente organizados para uma ação efetiva de combate às suas causas. Os procedimentos deverão incluir, no mínimo, a identificação da origem do incidente, dos indícios de intruso no sistema, das brechas conhecidas de segurança, da interrupção de serviço, etc. Na análise pós-incidente, deverá haver especificação e notificação do agente interno ou externo, de acordo com a natureza e categoria do evento ou incidente para aplicação das devidas medidas corretivas;

INSTALANDO mecanismos de detecção e prevenção projetados para proteger o Conglomerado CCB Brasil contra software de código malicioso e vírus. Esses controles deverão constar de todos os ativos relacionados à informação da empresa. Sob nenhuma hipótese os usuários tentarão pessoalmente erradicar ou limpar sua estação de trabalho após incidentes relacionados a código malicioso, devendo comunicar de imediato qualquer ameaça de vírus ou código malicioso detectado em computador da rede ou dispositivo relacionado;

MANTENDO-SE em conformidade com os acordos de licença de software, sendo que é expressamente proibida a aquisição e o uso de software não autorizado no Conglomerado CCB Brasil. Softwares antivírus deverão ser instalados e configurados em todos os computadores, PCs, laptops e demais dispositivos

móveis relacionados, além de servidores de rede, correio eletrônico e servidores de Internet para varredura de arquivos infectados, novos e antigos;

ASSEGURANDO que um canal de comunicação seja estabelecido, com atendimento em tempo integral, de forma eficiente e autônoma para atender e orientar nos casos de incidentes que possam colocar em risco a segurança das informações do Conglomerado CCB Brasil, bem como seu patrimônio. Todo incidente de segurança deverá ser imediatamente comunicado através desse canal;

COMPARTILHANDO, após aviso à Divisão de Segurança da Informação, os incidentes de segurança da informação com as partes interessadas e as instituições reguladoras. Isso também se aplica a incidentes comunicados por fornecedores/prestadores de serviços terceiros ou subterceirizados;

SEPARANDO funções e responsabilidades incompatíveis para minimizar a possibilidade de acesso ou uso indevido ou não autorizado a ativos relacionados à informação na Empresa ou seus processos comerciais. Da mesma forma, os ambientes de desenvolvimento de testes e produção igualmente deverão ser segregados estrategicamente para minimizar a possibilidade de modificações não autorizadas no ambiente de produção;

GARANTINDO o backup periódico dos ativos de informação para fins de recuperação operacional e conformidade com os planos de recuperação da continuidade dos negócios, sendo que tais backups devem ser retidos de acordo com os requisitos comerciais e regulatórios;

TESTANDO periodicamente a mídia usada nos backups quanto à sua confiabilidade e integridade. Os procedimentos para a restauração integral da informação deverão ser verificados periodicamente quanto à eficácia e desempenho. As mídias de armazenamento físico dos backups de documentos, dados do consumidor, clientes, administradores, colaboradores, informações de terceiros, mídias, incluindo correio eletrônico, devem seguir as diretrizes internas sobre retenção de informações do Conglomerado CCB Brasil;

DISPONIBILIZANDO espaço adequado para criar e manter os backups da informação, quando necessário. Os backups, que permaneçam no local, deverão ser armazenados em área física e ambientalmente protegida, com base nos requisitos de manuseio definidos na classificação da informação;

PROVENDO um sistema adequado para assegurar que todas as senhas padrão de equipamentos de rede sejam substituídas no momento da instalação. O Conglomerado CCB Brasil é responsável também por prover seus equipamentos

de um sistema adequado para gerenciamento de senhas de acesso e de sistemas, respeitando requisitos de complexidade, tamanho mínimo e histórico de senhas;

DISPONIBILIZANDO a todo usuário dos Serviços de Informação do Conglomerado CCB Brasil uma identificação exclusiva para autenticação e atribuição de responsabilidades individuais. Para que a identificação do usuário seja emitida, será requerida autorização documentada;

ADMINISTRANDO os privilégios de acesso aos sistemas segundo um processo formal durante o ciclo de vida, desde o registro até a revogação. O perfil dos usuários deverá ser estabelecidos de forma a alinhar os acessos de acordo com as necessidades específicas para o desempenho de suas respectivas funções;

RESTRINGINDO o acesso administrativo aos recursos do sistema ou privilégios similares apenas ao pessoal que execute a manutenção do sistema ou que tenha funções administrativas relacionadas. O acesso privilegiado deverá ser usado apenas para as tarefas administrativas do sistema;

ALINHANDO aplicativos ou qualquer outro recurso do Conglomerado CCB Brasil que hospedem ou forneçam acesso aos dados ou às normas internas aplicáveis de gerenciamento de senha. Os usuários aprovados e autorizados pelo Conglomerado CCB Brasil a utilizar os sistemas, redes, aplicativos e a informação ali contida, são responsáveis pela proteção de suas respectivas senhas. As senhas de usuários deverão permanecer confidenciais, não devendo, em hipótese alguma, ser compartilhadas, enviadas ou divulgadas de qualquer outra maneira.

ALERTANDO a todos os usuários, inclusive aqueles com acesso remoto aos sistemas do Conglomerado CCB Brasil, que eles são responsáveis pela segurança da conexão a todos os sistemas e recursos de informação da empresa. Em alinhamento com a estratégia e as diretrizes da Organização, o Conglomerado CCB Brasil não utiliza serviços em nuvem. Entretanto, fornecedores/prestadores de serviços diretos ou indiretos podem utilizar ambiente em nuvem para prestação de serviços desde que sigam os passos preestabelecidos nas diretrizes internas aplicadas à prática de segurança e gestão de riscos proporcional à relevância dos serviços. Todos deverão agir sempre conforme as diretrizes de Segurança da Informação do Conglomerado CCB Brasil para garantir a disponibilidade, a confidencialidade e a integridade das informações quando estiverem armazenadas, disponibilizadas e acessíveis em ambiente Cloud (Nuvem);

GARANTINDO que a criação de novos produtos, a seleção de mecanismos de segurança e a aquisição de bens ou serviços de tecnologia levem sempre em

consideração o balanceamento dos seguintes aspectos: risco, tecnologia, custo, qualidade, velocidade e impacto no negócio;

INCLUINDO as considerações de segurança em todas as fases do ciclo de vida do desenvolvimento dos sistemas, especialmente para assegurar que as políticas de segurança do Conglomerado CCB Brasil sejam abordadas em tempo hábil e com eficiência de custos;

IDENTIFICANDO, testando e documentando, antes de sua implantação, as aplicações e os sistemas de segurança para que não representem risco significativo. As equipes de Tecnologia da Informação devem formalizar uma análise de risco para cada novo aplicativo ou modificação importante em aplicativo executado pela Segurança da Informação. Os resultados deverão ser documentados e disponibilizados para uso posterior em testes de segurança e etapas de verificação;

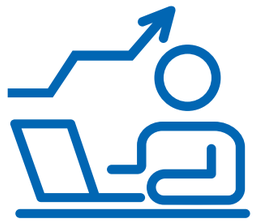
MANTENDO as bases dos processos de Segurança da Informação mesmo quando a responsabilidade for terceirizada para uma outra entidade, provendo auditorias periódicas e buscando reforçar a certificação de seu total cumprimento. Os requisitos de segurança do Conglomerado CCB Brasil relativos a partes externas devem ser abordados e documentados em contrato, com cláusulas contratuais estabelecidas sempre de acordo com os interesses das Políticas de Segurança da Informação, mantidas ou acessadas pelos fornecedores/prestadores de serviços na administração dos ativos de informação da Instituição;

ESTABELECENDO acordos de confidencialidade com os colaboradores, que serão solicitados a assinar documentação relacionada à segurança, a ser fornecida pelo Departamento de Recursos Humanos no ato da contratação. Tais documentos expressarão as responsabilidades gerais de segurança. Os colaboradores deverão ler com atenção, compreender e agir de acordo com os termos contratuais aplicáveis à sua posição. Para terceiros, o acordo de confidencialidade deve constar nos contratos entre as partes ou termo apartado;

DESENVOLVENDO e implantando uma estratégia abrangente de continuidade de negócios específica para os objetivos e prioridades da Empresa contra efeitos de falhas humanas ou técnicas ou desastres de grandes proporções. É fundamental, para a proteção adequada dos ativos de informação e processos de negócios críticos, que o Conglomerado CCB Brasil demonstre, por meio de testes preventivos e auditorias do processo de gestão, que possui capacidade de suporte adequada a eventuais necessidades de recuperação de suas atividades, de forma a retomar a normalidade no menor período de tempo possível;

IDENTIFICANDO e controlando os riscos na concessão de acesso de terceiros aos sistemas e ativos da informação do Conglomerado CCB Brasil. Nos casos em que houver necessidade de que consultores, parceiros comerciais, fornecedores/prestadores de serviços ou revendedores exerçam atividades e práticas de acesso, sob as bases dos contratos aplicáveis, o Conglomerado CCB Brasil reserva-se o direito de auditar e fazer inspeções on-site em prazos razoáveis de negócio;

PRESERVANDO a privacidade dos usuários, de maneira que todos os dados coletados por terceiros ou com terceiros compartilhados e que impliquem na identificação pessoal do usuário sejam devidamente comunicados e autorizados pelo proprietário da informação, salvo quando legalmente a autorização seja dispensada. Todas as informações coletadas e recebidas são utilizadas de acordo com a necessidade estritamente indicada na sua solicitação para prestação de serviços, sendo que existem controles implementados para proteger as informações contra acesso não autorizado ou processamento indevido.



QUAIS SÃO OS EFEITOS DA SEGURANÇA DA INFORMAÇÃO?

Ao determinar o respeito e o acompanhamento rigoroso do cumprimento de sua Política de Segurança da Informação, a alta direção do Conglomerado CCB Brasil garante que todos os seus colaboradores e fornecedores/prestadores de serviços atuem em conjunto no sentido de impedir a ocorrência de problemas com o sigilo das informações sob sua posse ou responsabilidade. Isso contribui efetivamente para a obtenção de resultados positivos nos negócios, preservando a qualidade e a credibilidade, além de dirimir riscos materiais ou perdas de reputação.

REFERÊNCIAS DESTE CONTEÚDO

Norma ISO/IEC 17799:2005, ABNT NBR ISO/IEC 27002:2013; Resolução CMN nº 4.893/2021; ISO/IEC 27.001; POG.09.110.

Gerenciamento de Riscos no Conglomerado CCB BRASIL

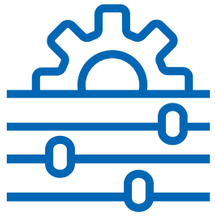
4.4.1 — COMO SE APLICA O GERENCIAMENTO DE RISCOS NO CONGLOMERADO CCB BRASIL?

Distribuída por toda a estrutura diretiva do Conglomerado CCB Brasil, o Gerenciamento de Riscos nasce no Conselho de Administração, passa pela Diretoria Executiva e chega ao Comitê de Riscos, que, coordenado pelo CRO, atua em cada uma das áreas da empresa. Sua função é preservar o ambiente de negócios, desenvolver e aprimorar ferramentas de controle e monitorar situações de crise, adotando indicadores tanto quantitativos como qualitativos para antecipar possíveis situações que possam provocar impactos negativos ou contrários aos interesses da Instituição.

Sempre alinhado aos objetivos estratégicos do Conglomerado CCB Brasil, o Gerenciamento de Riscos é um conjunto de ferramentas administrativas que dispõe de modelos e metodologias para a qualificação técnica dos processos que visam à prevenção e à identificação de eventuais riscos à integridade e à continuidade dos negócios da Instituição.

Por meio de políticas específicas, diretrizes de controle, prevenção e correção, o Gerenciamento de Riscos se dá por etapas distintas, localizando primeiramente os contextos sujeitos a riscos para, a partir dessa identificação, operar sua análise, tratamento e monitoramento.

Em função de sua importância estratégica e para dar maior especificidade às atribuições gerais, seguem aqui elencados os modos de funcionamento do Gerenciamento de Riscos por área:



NO CONSELHO DE ADMINISTRAÇÃO — O Conselho de Administração tem a responsabilidade de definir a estratégia, o apetite ao risco e a estrutura de controles para a Instituição, além de medir o desempenho dessa gestão em relação às metas:

DETERMINANDO a estrutura, as responsabilidades e os controles para gerenciar riscos e capital, e desenvolvendo e implantando uma estratégia corporativa de Enterprise-Wide Risk Management, de acordo com a tolerância a riscos da Instituição;

COMUNICANDO a estratégia de risco, as principais políticas para sua implantação e a estrutura de Gerenciamento de Riscos para toda a Instituição:

Para mais informações, acesse: http://www.br.ccb.com/menu/Institucional/Governanca-Corporativa/Gestao-de-Riscos/Relatorios-de-Gerenciamento-de-Risco-109

MONITORANDO tendências e potenciais desenvolvimentos do mercado que possam ser significativos no que tange ao Gerenciamento de Riscos e de Capital, e, caso haja necessidade, realizando e propondo mudanças nas estratégias de risco da Instituição;

DEFININDO, em caso de exceções às políticas estabelecidas e/ou aos limites monitorados, os procedimentos específicos e alçadas de aprovação necessárias, considerando as medidas a serem tomadas em caso de violação de qualquer limite predefinido;

ESTABELECENDO e revisando, em conjunto com o Comitê de Riscos, o(a) CRO e os demais membros da Diretoria, os níveis de apetite ao risco expressos na Declaração de Apetite ao Risco (RAS);

APROVANDO e revendo, com periodicidade mínima anual, as políticas, estratégias e limites de Gestão de Riscos, as políticas e estratégias de Gerenciamento de Capital, o Programa de Teste de Estresse, as Políticas de Gerenciamento de Continuidade de Negócios, o Plano de Contingência de Liquidez, o Plano de Capital e o Plano de Contingência de Capital;

ASSEGURANDO a aderência da Instituição às Políticas de Gerenciamento de Risco, suas estratégias e limites;

PROPONDO a pronta correção de eventuais deficiências nas estruturas de Gerenciamento de Riscos e de Capital;

APROVANDO mudanças relevantes, induzidas a partir dos riscos, nas políticas e estratégias de Gerenciamento de Riscos, bem como nos sistemas, rotinas e procedimentos;

AUTORIZANDO, quando necessário, exceções a políticas, procedimentos, limites e níveis de apetite ao risco expressos nas RAS;

ASSEGURANDO adequação e suficiência de recursos para um independente, objetivo e efetivo desempenho das atividades relacionadas ao Gerenciamento de Riscos e de Capital;

CUIDANDO para que a estrutura de remuneração da Instituição não incentive comportamentos inconsistentes com os níveis de apetite ao risco expressos na RAS e para que os níveis de capital e liquidez sejam adequados e suficientes;

ESTABELECENDO as atribuições do Comitê de Riscos e disseminando a cultura de risco na Instituição.

NA DIRETORIA EXECUTIVA — A Diretoria Executiva define estratégias para orientar atividades e estruturas alinhadas com os valores do Conglomerado. As decisões colegiadas são tomadas por intermédio do Comitê da Diretoria Executiva (CDE), que se reúne ao menos todo mês ou sempre que convocado, sendo que seus diretores atuam:

DESENVOLVENDO e implantando a estratégia corporativa de Gerenciamento de Riscos e de Capital de acordo com a tolerância ao risco definida pelo Conselho de Administração;

DETERMINANDO a estrutura de Gerenciamento de Riscos na Instituição e as responsabilidades e controles para o Gerenciamento de Riscos e de Capital;

COMUNICANDO a estratégia de risco e as principais políticas de implementação;

MONITORANDO as tendências atuais e os potenciais avanços do mercado que possam ser significativos no que tange ao Gerenciamento de Riscos e propondo e realizando mudanças nas estratégias de risco da Instituição, caso haja necessidade;

DEFININDO, em caso de exceções às políticas definidas e/ou aos limites monitorados, os procedimentos específicos e alçadas de aprovação necessárias, considerando as medidas a serem tomadas em caso de violação de qualquer limite predefinido;

PARTICIPANDO de reuniões e convocando-as, caso necessário, de forma a monitorar, identificar, avaliar e mitigar riscos, levando em consideração o contexto do ambiente de controle existente. Documentando sempre todas as decisões relacionadas à ação mitigadora requerida ou à aceitação de riscos relevantes. Aprovando, quando necessário, as políticas e procedimentos relacionados ao Gerenciamento de Riscos e de Capital;

SUPERVISIONANDO e gerenciando o apetite ao risco do Banco de modo satisfatório, em linha com o apetite ao risco geral do Grupo;

RELATANDO o evento de risco material para o Head Office e organizando respostas e soluções oportunas e necessárias para eventos de risco no nível gerencial. Revisando com periodicidade semestral o relatório abrangente de gerenciamento de riscos do Banco.

NO COMITÊ DE RISCO — O Comitê de Riscos se reporta ao Head Office da Instituição. É sua responsabilidade atuar:

PROPONDO recomendações ao Conselho de Administração pelo menos uma vez por ano;

AVALIANDO os níveis de apetite ao risco documentados na RAS, bem como estratégias para sua gestão, considerando os riscos tanto individualmente quanto de forma integrada;

SUPERVISIONANDO a conduta e desempenho do CRO e a observância, pela Diretoria da Instituição, dos termos da RAS;

AVALIANDO a aderência dos processos de Gerenciamento de Riscos ao que foi estabelecido como política e mantendo registros de suas próprias deliberações e decisões;

MONITORANDO o ambiente externo de negócios no Brasil e na América Latina, analisando a eficácia do Gerenciamento de Riscos e Controles Internos, bem como eventos de risco relevantes no mercado local.

FORNECENDO sugestões para solucionar ou mitigar os impactos de eventos de risco e analisando outros tópicos específicos sob sua responsabilidade;

ORGANIZANDO a reunião do Comitê de Risco mensalmente ou em caráter extraordinário, se necessário, realizando a qualificação de seus membros e garantindo que as atas das reuniões cumpram com os requisitos regulamentares e as diretrizes do Head Office.

NA POSIÇÃO DE CRO — O(A) Chief Risk Officer é um(a) profissional diretamente subordinado(a) ao Head Office cujas responsabilidades são proceder:

SUPERVISIONANDO a constante implementação e desenvolvimento de estruturas de gestão de risco, inclusive suas melhorias;

IMPLEMENTANDO políticas, processos, relatórios, sistemas e modelos compatíveis com a RAS e os objetivos estratégicos, e promovendo o mecanismo colaborativo no controle de riscos, de acordo com as instruções e orientações do Head Office;

REUNINDO-SE com o Head Office e a ele se reportando periodicamente para atender aos seus requisitos de qualificação de acordo com a regulamentação e as diretrizes técnicas;

FORNECENDO treinamento adequado em políticas, processos, relatórios, sistemas e modelos, mesmo quando esses modelos forem desenvolvidos por terceiros para a equipe de Risco. Ao(À) CRO não é permitido responder simultaneamente por nenhum departamento comercial;

OFERECENDO subsídios e participando de processos estratégicos de tomada de decisão relacionados ao Gerenciamento de Riscos e, quando aplicável, ao Gerenciamento de Capital, como assistência ao Conselho de Administração;

ORGANIZANDO e coordenando continuamente os estudos necessários para o aperfeiçoamento do controle e do Gerenciamento de Riscos do CCB Brasil.

QUAIS SÃO OS EFEITOS DO GERENCIAMENTO DE RISCOS?

O Gerenciamento de Riscos do Conglomerado CCB Brasil aqui descrito resulta na proteção efetiva dos ativos da Instituição nos diversos contextos de risco a que está exposta: crédito, operacional, de mercado, etc. Tais políticas criam um ciclo virtuoso que elimina perdas e abalos nas operações. Além disso, sua prática atenta aos mínimos detalhes também colabora para a estruturação plena dos mecanismos de aferição, controle e implantação de políticas e estratégias de negócio com segurança e alta performance.

4.4.2 — GERENCIAMENTO DE RISCOS OPERACIONAIS

O QUE É RISCO OPERACIONAL?

Chamamos risco operacional qualquer possibilidade de ocorrência de perdas resultantes de eventos externos imprevistos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas.

O risco operacional pode estar associado à eventual inadequação ou incorreção em contratos firmados, pode estar ligado às sanções em razão do descumprimento de dispositivos legais, ou pode ainda estar relacionado às indenizações por danos a terceiros decorrentes de atividades imprevidentes desenvolvidas por algum colaborador.

O risco operacional pode comprometer os objetivos e a eficiência dos serviços prestados, a qualidade dos produtos oferecidos e até a própria existência das empresas envolvidas. A eficiência dos procedimentos operacionais e o rigor dos controles internos na prestação de serviços reduzem consideravelmente a probabilidade de ocorrência de um evento de risco operacional. Da mesma forma podem mitigar seus eventuais impactos, caso já tenham ocorrido. Para isso, há a necessidade do envolvimento de todos os agentes, externos e internos, para seu efetivo controle.

QUAIS SÃO AS CAUSAS DOS RISCOS OPERACIONAIS?

Os fatores geradores dos riscos operacionais são as fragilidades e as vulnerabilidades internas ou externas que possibilitam sua materialização. As causas podem ser creditadas a falhas de:

PESSOAS — quando da ausência de conduta ética ou incompetência no desempenho de suas atribuições;

SISTEMAS — quando de algum erro da infraestrutura e arquitetura de TI ou falta de disponibilidade para armazenamento e processamento de rede;

PROCESSOS — quando da desobediência das normas definidas pela organização — seus fluxos, suas etapas de desenvolvimento, suas normas internas — ou da não aderência à legislação vigente;

AMBIENTE EXTERNO — quando da ocorrência de imprevistos no ambiente social de negócios ou no ambiente regulatório do país.

COMO GERENCIAR O RISCO OPERACIONAL?

O adequado gerenciamento do risco operacional está diretamente relacionado ao conhecimento dos processos internos existentes na empresa. Desse modo, a empresa deve manter-se permanentemente atualizada, especialmente em relação aos processos considerados críticos, mantendo seus riscos operacionais identificados, avaliados, monitorados e controlados. Para isso, deve

IDENTIFICAR os riscos operacionais que possam impactar os objetivos estratégicos da Instituição, incluindo os fatores geradores (causas) e possíveis impactos do risco operacional identificado;

MENSURAR e determinar o efeito potencial do risco operacional em relação à probabilidade de ocorrência e ao seu impacto;

AVALIAR as opções de tratamento dos riscos operacionais, realizar análises adicionais para melhor compreender os riscos operacionais e manter atualizados os controles existentes.

MONITORAR eventuais deficiências do processo de gestão do risco operacional;

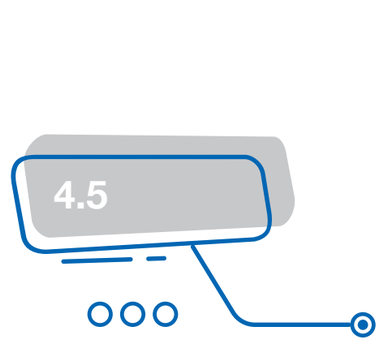
REPORTAR e divulgar as informações sobre riscos operacionais e controles, permeando as esferas da Instituição, mercado e órgãos reguladores;

CONTROLAR e registrar o comportamento dos riscos operacionais, limites, indicadores e eventos de perda operacional, bem como implementar mecanismos de forma a garantir que os limites e indicadores de risco operacional permaneçam dentro dos níveis definidos;

CRIAR e implementar mecanismos para mitigar o risco operacional, buscando reduzir as perdas a zero.

REFERÊNCIAS DESTE CONTEÚDO

Bank For International Settlement (BIS). Sound Practices for the Management and Supervision of Operational Risk; Resolução CMN nº 4.557; Instituto Brasileiro de Governança Corporativa (IBGC). Gerenciamento de Riscos Corporativos; ISO 31.000:2018. Gestão de Riscos — Diretrizes; ISO 31.010:2012. Gestão de Riscos — Técnicas para o Processo de Avaliação de Riscos; ISO Guia 73. Gestão de Riscos — Vocabulário; COSO — Gerenciamento de Riscos Corporativos — Estrutura Integrada.



Gestão de Continuidade nos Negócios no Conglomerado CCB BRASIL

Sobre a continuidade dos negócios e outras responsabilidades administrativas.

O QUE É GESTÃO DE CONTINUIDADE NOS NEGÓCIOS?

A gestão de continuidade dos negócios é o comprometimento em manter suas operações, antes, durante e após um incidente, minimizando os efeitos causados pela indisponibilidade das suas operações ou seus impactos financeiros, legais e regulatórios decorrentes de um incidente materializado em seus ativos críticos como recursos humanos, processos e tecnologias essenciais para o funcionamento de suas operações.

A ISO 22301 é a norma internacional para gestão de continuidade dos negócios e se baseia no sucesso da norma britânica BS 25999 e de outras normas regionais. Ela foi criada para proteger os negócios de possíveis intercorrências que possam impedir a Empresa de atingir seus objetivos. São considerados incidentes de interrupção desde condições meteorológicas adversas e extremas, incêndios, inundações, desastres naturais até roubo, interrupções nos serviços de TI, doença dos funcionários, ataques terroristas, etc.

PARA QUE SERVE A GESTÃO DE CONTINUIDADE NOS NEGÓCIOS?

O sistema de Gestão de Continuidade nos Negócios, por meio da norma ISO 22301, permite identificar ameaças relevantes à Empresa e quais funções críticas de negócios poderão ser afetadas. Isso permite que se implementem os planos antecipadamente, garantindo que os negócios não sejam interrompidos. Suas ações incluem:

IDENTIFICAR e gerenciar ameaças atuais e futuras aos seus negócios;

ADOTAR uma atitude proativa para minimizar o impacto de incidentes implementando e operando controles e medidas para a gestão da capacidade de gerenciamento dos eventuais incidentes de interrupção;

MANTER funções críticas em funcionamento durante períodos de crise;

MINIMIZAR o tempo de inatividade durante incidentes e melhorar o tempo de recuperação.

COMO SE APLICA A GESTÃO DE CONTINUIDADE NOS NEGÓCIOS NO CONGLOMERADO CCB BRASIL?

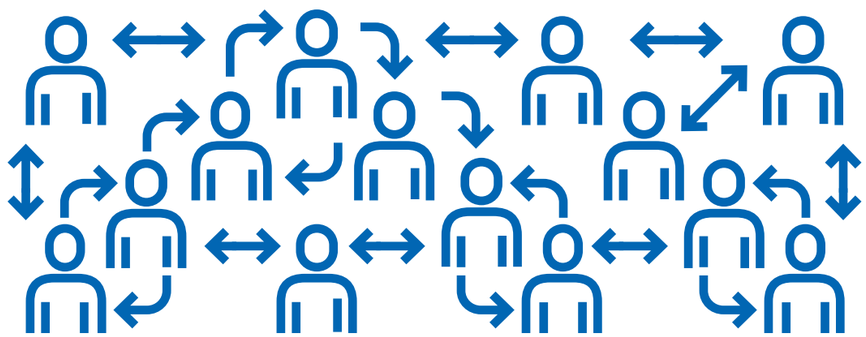
É fundamental, para a proteção adequada dos ativos de informação e processos de negócios críticos, que o Conglomerado CCB Brasil demonstre, por meio de testes preventivos e auditorias do processo de gestão, possuir capacidade de suporte adequada a eventuais necessidades de recuperação de suas atividades, de forma a retomar a normalidade no menor período de tempo possível.

O Conglomerado CCB Brasil possui políticas e procedimentos para apoiar ações e atividades associadas à Gestão de Continuidade dos Negócios. Os planos apresentam um conjunto de procedimentos detalhados a serem seguidos pelas equipes de apoio a contingências, concentrando-se em cada uma delas em diferentes situações.

Durante os momentos de recuperação (início da contingência) e restauração (retorno à normalidade), revisita-se periodicamente a documentação de suporte para a execução de atividades e procedimentos críticos a fim de refletir os papéis e as responsabilidades dos times envolvidos no processo de Continuidade nos Negócios.

Para atendimento do Plano de Gestão de Continuidade nos Negócios, são realizados exercícios periódicos para garantir que, em situação real de contingência, o Conglomerado CCB Brasil mantenha suas operações durante a crise.

Esses exercícios são estruturados inicialmente considerando a priorização dos processos críticos contidos no Business Impact Analysis Report (BIA) do Conglomerado CCB Brasil, sendo que funcionários-chave são convocados para deles participarem a fim de testar a executabilidade de suas tarefas de rotina em busca da preservação de ativos críticos, recursos humanos, processos e tecnologias essenciais para o funcionamento das operações.



QUAIS SÃO OS EFEITOS DA GESTÃO DE CONTINUIDADE NOS NEGÓCIOS?

Com a aplicação das boas práticas de Gestão de Continuidade nos Negócios no Conglomerado CCB Brasil, consegue-se:

(Operacional)
EVITAR a interrupção total ou parcial das atividades da Instituição;

(Financeiro)
EVITAR pagamentos de multas, indenizações, custas e honorários judiciais; reembolso por cobranças indevidas; perdas ou prejuízos nas operações em razão de falhas ou fraudes; entre outros;

(Legal)
EVITAR sanções legais impedindo a prestação de serviços ou o funcionamento da Instituição, processos administrativos, cíveis, tributários ou trabalhistas; entre outros;

(Imagem)
EVITAR uma percepção negativa da imagem da Instituição por parte de seus clientes, mídias, contrapartes, entre outros stakeholders.

REFERÊNCIAS DESTE CONTEÚDO

ISO 31.000 de 2009; ISO/IEC 22302; Resolução CMN nº 4.557; POG.05.004
Fonte: https:// www.bsigroup.com/pt-BR/ISO-22301-Continuidade-dos Negocios/ Introducao-a-ISO-22301/

4.6

Programa de Prevenção a Atos Ilícitos no Conglomerado CCB BRASIL

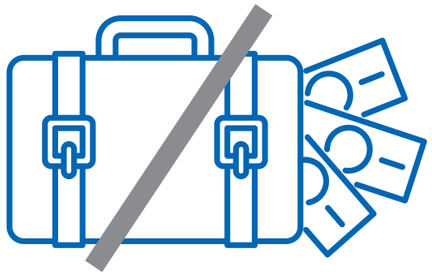
Sobre os compromissos de integridade.

O QUE SÃO ATOS ILÍCITOS?

Na prática, podemos dizer que é toda e qualquer ação de desobediência às prescrições legais, seja ela no âmbito cível ou no âmbito penal. No ambiente do sistema financeiro, há vários tipos de fraude, facilitação ou acobertamento de crimes que constituem ato ilícito, em sua maioria envolvendo lavagem de dinheiro, corrupção, terrorismo ou tráfico de drogas.

O QUE É E PARA QUE SERVE O PROGRAMA DE PREVENÇÃO A ATOS ILÍCITOS?

Todos os princípios que balizam o Código de Ética e Conduta do Conglomerado CCB Brasil — consideração pelos outros, compromisso com a transparência, observância das leis e responsabilidade social corporativa — apontam para a necessidade de se atuar com firmeza na prevenção a atos ilícitos.



As instituições financeiras, por portarem grande volume de ativos advindos de transações ao redor do globo, têm condições de auxiliar as diversas autoridades de controle da criminalidade no rastreamento legal e na comunicação de suspeição de atividades ou operações que apresentem indícios de lavagem de dinheiro, corrupção, financiamento ao terrorismo ou tráfico de drogas.

A prevenção a atos ilícitos se dá por meio de um conjunto de ferramentas indispensáveis para a proteção das próprias instituições financeiras, que contam com a adesão de todos os públicos de interesse do Conglomerado CCB Brasil. A observância e o cumprimento das Diretrizes do Programa de Integridade e Política de Prevenção a Lavagem de Dinheiro e Ilícitos têm sua aplicação indistinta para todos os níveis hierárquicos do CCB Brasil — administradores, colaboradores, terceiros, fornecedores/prestadores de serviço.

QUAIS SÃO AS SANÇÕES LEGAIS PREVISTAS PARA ATOS ILÍCITOS?

O Conselho de Segurança da Organização das Nações Unidas (ONU) é o principal responsável pela manutenção da paz e segurança mundial. De acordo com a Carta das Nações Unidas, todos os Estados-Membros são obrigados a cumprir as decisões do Conselho. Esse conselho assume a liderança na determinação da existência de uma ameaça à paz ou ato de agressão. Convida as partes em uma controvérsia a resolvê-la por meios pacíficos e recomenda métodos de ajuste ou termos de solução. Em alguns casos, o Conselho de Segurança pode recorrer à imposição de sanções ou mesmo autorizar o uso da força para manter ou restaurar a paz e a segurança internacionais. As sanções têm por objetivo exercer pressão sobre um Estado ou entidade para cumprir os objetivos fixados pelo Conselho de Segurança, sem recorrer ao uso da força. As sanções, portanto, oferecem ao Conselho de Segurança um instrumento importante para fazer cumprir suas decisões. No Brasil, a Lei nº 13.810, de 8 março de 2019, conhecida como Lei de Congelamento de Ativos, estabelece a indisponibilidade dos recursos de pessoas ou empresas ligadas ao terrorismo, conforme lista fornecida pela ONU.

A União Europeia (UE) também possui uma extensa lista de sanções para quando se faz necessário intervir na prevenção de conflitos, situações emergenciais e crises humanitárias. Entre as represálias, estão o embargo de armas e munições, a proibição de comércio internacional e a restrição de circulação ou bloqueio de ativos, podendo atingir governos, entidades e indivíduos. A promoção da paz e segurança internacional; a prevenção de conflitos; o apoio à democracia, ao Estado de direito e aos direitos humanos; e a defesa dos princípios do direito internacional são os principais objetivos almejados com essas tratativas

Do mesmo modo, o Tesouro Americano impõe rígidas sanções por meio de seu Office Foreign Assets Control (OFAC), ou Agência de Controle de Ativos Estrangeiros dos Estados Unidos. Tais sanções são aplicáveis a países, indivíduos ou entidades que infrinjam regras de comércio internacional, que estejam ligados a crimes de terrorismo ou tráfico internacional de drogas, que desenvolvam atividades relacionadas à proliferação de armas de destruição em massa ou que exerçam qualquer ameaça que coloque em risco a segurança nacional ou a política econômica dos Estados Unidos da América.

O Foreign Corrupt Practices Act (FCPA), ou Lei contra Práticas de Corrupção no Exterior, é uma lei norte-americana anticorrupção no estrangeiro que foi promulgada pelo Congresso dos EUA em 1977. Ela cria sanções cíveis, administrativas e penais no combate à corrupção comercial internacional e se aplica a pessoas físicas e empresas americanas que, em atividade comercial no exterior, utilizem-se de corrupção no poder público estrangeiro para obter ou reter transações comerciais naquele país.

A United Kingdom Bribery Act (UKBA), ou Lei Anticorrupção do Reino Unido, de 2011, é considerada uma das leis de combate à corrupção mais rígidas do mundo, punindo, inclusive, a corrupção privada. Assim como as principais leis anticorrupção existentes, ela também possui a chamada extraterritorialidade, ou seja, é aplicável não apenas às empresas britânicas que operam no mercado local e/ou em mercados estrangeiros, mas também às sociedades estrangeiras que atuam no Reino Unido, além de prever a punição de pessoas físicas e jurídicas pelo cometimento de um dos quatro crimes principais contidos no texto legal. As multas aplicáveis às pessoas físicas e jurídicas são ilimitadas, sendo que, no caso de pessoas físicas, a multa pode ser aplicada de forma cumulativa ou isolada com a penalidade de prisão, que pode ser de até 10 (dez) anos. Os diretores das empresas envolvidas em corrupção podem ser destituídos do cargo e sofrer processos de impedimento, acarretando a proibição de atuar na função por até 15 (quinze) anos. A falha na prevenção de subornos foi também tipificada como crime corporativo no Reino Unido.

No caso do Brasil, o governo criou, em 1998, uma unidade de inteligência financeira, o Conselho de Controle de Atividades Financeiras (COAF). Nessa mesma data, tipificou-se a lavagem de dinheiro por meio da Lei nº 9613/98 (com alterações introduzidas pela Lei nº 12.683/12), que dispõe sobre a prevenção da utilização do sistema financeiro para ilícitos. Assim, ficou caracterizado como crime ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes direta ou indiretamente de infração penal.

O GAFI/FATF, por sua vez, desenvolve padrões e a promoção da efetiva aplicação das medidas legislativas, regulamentares e operacionais contra a lavagem de dinheiro, o financiamento do terrorismo, a proliferação de armas de destruição em massa e outras ameaças à integridade do sistema financeiro internacional. Em 2013, foi promulgada no Brasil, a Lei do Crime Organizado, que não apenas tipifica, dentro do contexto de lavagem de dinheiro, o que é uma organização criminosa, mas também define os processos de investigação criminal, meios de obtenção de prova, infrações penais correlatas e procedimento criminal.

A Lei Federal brasileira n° 12.846/2013, conhecida como “Lei Anticorrupção”, veio como um marco na legislação de proteção da administração pública e, por via indireta, de toda a sociedade, ao estabelecer, em normativo próprio e específico, a responsabilização objetiva, civil e administrativa das pessoas jurídicas pela prática de atos contra a administração pública nacional e estrangeira.

PREVENÇÃO A ATOS ILÍCITOS

A Lei é aplicável às sociedades empresárias, sociedades simples, personificadas ou não, fundações, associações de entidades ou pessoas, bem como sociedades estrangeiras, que tenham sede, filial ou representação no território brasileiro, constituídas de fato ou de direito, ainda que temporariamente, prevendo a responsabilização objetiva, civil e administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.

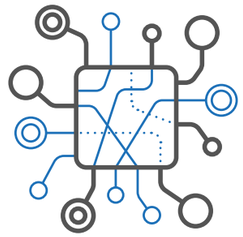
Em 2015, o Decreto Federal nº 8.420/2015, revogado em 2022 pelo Decreto nº 11.129, regulamentou tal legislação, pormenorizando os mecanismos e procedimentos de integridade, auditoria, aplicação de códigos de ética e conduta e incentivos de denúncia de irregularidades que devem ser adotados pelas empresas e que podem ser alvo de inspeção pela Controladoria Geral da União (CGU). Segundo o documento, o programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e riscos atuais das atividades de cada pessoa jurídica, a qual, por sua vez, deve garantir seu constante aprimoramento e adaptação.

Em linha com as boas práticas de governança corporativa, em 2016, a International Organization for Standardization (ISO) publicou a norma ISO 37001:2016 – Sistemas de Gestão Antissuborno, para apoiar as organizações a combater o suborno, por meio de uma cultura de integridade, transparência e conformidade com as leis e regulamentações aplicáveis, através dos seus requisitos, políticas, procedimentos e controles adequados para lidar com os riscos de suborno.

Ainda nesse ano, na esteira das mesmas precauções, veio a Lei Antiterrorismo, que, além de tipificar os crimes de terrorismo e prática de organização terrorista, estabelece igualmente as penalidades cabíveis, visando a um controle ainda maior sobre os atos ilícitos.

Nesse mesmo passo, consolidando os princípios, regras e as melhores práticas nacionais e internacionais de ética e integridade para Prevenção à Corrupção e a

outros atos lesivos à Administração Pública nacional ou estrangeira, a autorregulação bancária da Federação Brasileira de Bancos (FEBRABAN), em 2019, instituiu normativo descrevendo os principais pilares para estruturação e melhoria contínua do Programa de Integridade das Instituições Financeiras Signatárias.



COMO SE APLICA O PROGRAMA DE PREVENÇÃO A ATOS ILÍCITOS NO CONGLOMERADO CCB BRASIL?

Consolidando os princípios, regras e as melhores práticas nacionais e internacionais de ética e integridade para Prevenção à Corrupção e a outros atos lesivos à Administração Pública nacional ou estrangeira, o Programa de Integridade do Conglomerado CCB Brasil é constituído de um conjunto de diretrizes corporativas para atendimento à Lei Federal nº 12.846, de 1° de agosto de 2013 e ao Normativo do SARB N° 021/2019.

É fundamental que todos tenham consciência da importância da prevenção à lavagem de dinheiro, corrupção, financiamento do terrorismo e tráfico de drogas quanto aos riscos legais e de imagem aos quais o Conglomerado CCB Brasil pode se expor. Por isso, cabe ressaltar a responsabilidade de cada um no desempenho de suas funções no sentido de se evitar ou mitigar a ocorrência da utilização do Conglomerado CCB Brasil em atos ilícitos.

Há no Conglomerado equipes dedicadas exclusivamente à prevenção da utilização da Instituição para atividades ilegais ou impróprias, bem como associação da imagem do Conglomerado CCB Brasil à prática e/ou facilitação de atos ilícitos.

O Conglomerado CCB Brasil, com o apoio da Alta Administração, promove medidas educativas quanto aos valores éticos expressados no seu Código de Ética e Conduta, com o intuito de aproximar o grau de aderência ao Programa e transparência nas relações com seus públicos de relacionamento. Além disso,

mantém plataforma de treinamentos para os colaboradores e, quando necessário, ministra treinamentos presenciais sobre o Programa de Integridade.

Mantém também um canal de denúncia para que toda e qualquer situação que supostamente envolva ou caracterize descumprimento do Código de Ética e Conduta do Conglomerado CCB Brasil possa ser direcionada aos meios de acesso elencados abaixo:

E-mail externo:
comite.etica@br.ccb.com

E-mail interno:
Comitê de Ética

Site da Instituição:
www.br.ccb.com/Fale-Conosco;

Canal interno disponibilizado na intranet
no ponteiro “Ética” (restrito aos funcionários):
Fale com o Comitê de Ética.

Os procedimentos para apuração, encaminhamento e tratamento de infrações, incluindo as deliberações necessárias para aplicação de sanções aos infratores, são formalizados em procedimentos internos específicos para apuração de infrações éticas.

Para o pleno atendimento da Resolução CMN nº 4.859 de 23 de outubro de 2020, do BACEN, que estabelece a obrigatoriedade de um Canal de Denúncia, para tratamento das demandas, manifestações e registros nesse sentido, a Empresa disponibiliza: www. br.ccb.com/denuncia e www.ccbfinanceira.com.br/atendimento/canal-de-denuncia.php. Trata-se de uma via constantemente aberta a todos os funcionários, colaboradores, terceiros, clientes, usuários, parceiros ou fornecedores do Conglomerado CCB Brasil.

Quanto às medidas disciplinares e procedimentos para garantir a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados, reforçamos que qualquer suspeita ou violação deve ser reportada, tempestivamente, ao Comitê de Ética que analisará e deliberará sobre penalidades de acordo com a gravidade.

Portanto, todos os representantes da Instituição, colaboradores, estagiários e quaisquer terceiros, diretos ou indiretos, temporários, fornecedores/prestadores de serviço, consultores, assessores e agentes, contratados ou subcontratados declaram e garantem mutuamente:

NÃO pagar, oferecer, autorizar e/ou prometer — direta ou indiretamente — toda e qualquer quantia, bem de valor ou vantagem indevida a qualquer pessoa que seja oficial, agente, colaborador ou representante de qualquer governo, nacional ou estrangeiro, ou de suas agências e organismos nacionais ou internacionais, ou a qualquer partido político, candidato ou ocupante de cargo público ou a escritórios de partidos políticos, ou a qualquer outra pessoa;

NÃO oferecer dados ou receber vantagem ou favorecimento com a finalidade de obter ou manter tratamento diferenciado indevido, em violação às leis que versam sobre crimes e práticas de corrupção e contra a administração pública, observando sempre as leis de prevenção à lavagem de dinheiro e de combate ao financiamento de terrorismo, tráfico de drogas e corrupção;

NÃO se eximir de observar e respeitar a Política Corporativa Anticorrupção e o Código de Ética e Conduta do Conglomerado CCB Brasil de forma atenta e total;

NÃO aceitar, a qualquer tempo e sob qualquer ônus, nenhum tipo de relacionamento envolvendo países que possuam embargos e/ou restrições na OFAC ou pessoas físicas ou jurídicas elencadas ou que venham a ser elencadas na Specially Designated Nationals and Blocked Persons List (SDN), ou Lista de Cidadãos com Designação Especial e Pessoas Suspensas, da OFAC; ou que estejam na lista da ONU; ou na lista da UE; ou que estejam restritas pelas leis brasileiras, devendo, nesses casos, informar aos envolvidos os motivos da recusa.

QUAIS SÃO OS EFEITOS DA PREVENÇÃO A ATOS ILÍCITOS?

Os procedimentos e as boas práticas aqui descritas possibilitam o aumento da probabilidade de detecção de suborno, os chamados crimes do colarinho branco, e o rastreamento de associação a diversos outros crimes, com efetivo sucesso nos processos judiciais associados, diminuindo drasticamente os riscos de perda de ativos e graves danos reputacionais.

A principal decorrência do rígido controle de eventuais indícios de atos ilícitos no Conglomerado CCB Brasil é a eliminação de riscos de conformidade legal e operacional, como penalidades nacionais e internacionais que possam vir a prejudicar a imagem da Instituição.

Atuando sempre com base nesse firme posicionamento de conformidade legal e pela força de seus princípios éticos estabelecidos, o Conglomerado CCB Brasil acredita que os bancos, como entidades que controlam boa parte da circulação de moeda no planeta, funcionam como importante ferramenta na construção de uma sociedade mais justa e menos desigual.

REFERÊNCIAS DESTE CONTEÚDO

Lei nº 12.846/13; Decreto nº 11.129/22; Normativo SARB nº 11, de 1º de agosto de 2013; Normativo SARB nº 021, de 13 de março de 2019; Lei nº 9.613/98; Lei nº 13.260/16; Lei nº 13.810/19; Resolução BCB 44/2020; Circular BCB nº 3.978/2020; Cayman/FATCA/CRS/FCPA/UKBA Legislation.

4.7

Autorregulação Bancária no Conglomerado CCB BRASIL

Sobre os códigos normativos estabelecidos em conjunto pelo setor.

O QUE É A AUTORREGULAÇÃO?

A autorregulação ou a autorregulamentação é uma forma inteligente e ampla de se estabelecer um padrão de conduta normativa de acordo com os interesses de cada instituição, segundo referenciais comuns a outras instituições. Esses referenciais vão desde a definição de posturas legais nos âmbitos da condução ética dos negócios, da proteção ao consumidor, das responsabilidades socioambientais e de governança corporativa até as recomendações mais severas para a prevenção de ilícitos.

PARA QUE SERVE A AUTORREGULAÇÃO?

Os eixos normativos desse conjunto de regras aplicáveis foram criados pela Federação Brasileira de Bancos (FEBRABAN), e o Conglomerado CCB Brasil, como instituição financeira associada, aderiu aos compromissos ali estabelecidos, de forma comum a todo o sistema bancário, como um Código de Regulamentação do setor.

COMO SE APLICA A AUTORREGULAÇÃO NO CONGLOMERADO CCB BRASIL?

O cumprimento das regulamentações vigentes, bem como das diretrizes previstas nesta política e nos demais normativos internos do Banco, é periodicamente monitorado e fiscalizado, tanto interna como externamente. Os casos de descumprimento destas normas são considerados infrações e estão sujeitos, sem prejuízo das responsabilidades do Comitê de Ética, a penalidades, medidas coercitivas e meios alternativos de solução de controvérsias aplicáveis às instituições financeiras, a outras instituições supervisionadas pelo Banco Central do Brasil e aos integrantes do Sistema de Pagamentos Brasileiro. Tais fatos serão sempre contemplados no Relatório de Conformidade, emitido periodicamente.

Para fins didáticos, a FEBRABAN tratou a autorregulação por temas distintos e sempre atualizados na rede em documentos específicos. A ideia é promover uma concorrência saudável e ética no mercado e assegurar uma atuação livre, esclarecida e consciente de parte a parte. Destacam-se aqui, de forma geral, o que você vai encontrar em cada uma das normativas vigentes no texto do Sistema de Autorregulação Bancária (SARB):

Código de Conduta Ética e Autorregulação Bancária — Estabelece os valores e princípios que regem o documento: integridade, equidade, respeito ao consumidor, transparência, excelência, sustentabilidade e confiança. Detalha as responsabilidades e os compromissos firmados pelas instituições signatárias, a abrangências das normas apresentadas e as competências gerais dos conselhos, diretorias e comissões.

SARB nº 001/2008 — Sobre o RELACIONAMENTO COM O CONSUMIDOR PESSOA FÍSICA: I. no atendimento realizado no terminal de autoatendimento, internet, dispositivos móveis de comunicação, central de atendimento e ouvidoria; II. na oferta e publicidade dos seus produtos e serviços; III. nos procedimentos para a contratação com seus consumidores; e IV. no sigilo e segurança dos serviços.

SARB nº 002/2008 — Sobre as NORMAS DE CONTA CORRENTE. Apresenta regras básicas sobre movimentação, cobrança de tarifas e pacote de serviços, e relata os riscos, medidas de segurança e controle para a utilização dos serviços, oferecendo ainda uma panorâmica sobre a importância de informações cadastrais precisas e a necessidade de atualização, detalhando inclusive os eventuais efeitos de sua desatualização.

SARB nº 003/2008 — Sobre o SERVIÇO DE ATENDIMENTO AO CONSUMIDOR (SAC). Trata da definição do SAC no âmbito legal e dos objetivos dessa prestação de serviços, desde a disponibilidade do acesso ao atendimento, da qualidade do serviço e de seu aperfeiçoamento até o acompanhamento das demandas dentro dos prazos estabelecidos.

SARB nº 004/2009 — Sobre o ATENDIMENTO AO CONSUMIDOR NAS AGÊNCIAS. Trata dos pontos de atendimento físico, das informações, dos produtos e dos serviços ali disponíveis. Cuida do atendimento prioritário, da acessibilidade e da qualidade do atendimento. Além disso, aborda os horários de funcionamento, os guichês de recebimento, as ouvidorias e os canais alternativos de atendimento, entre outras exigências.

SARB n° 005/2009 — Sobre a oferta e contratação de CRÉDITO DIRETO AO CONSUMIDOR E ARRENDAMENTO MERCANTIL FINANCEIRO PARA A AQUISIÇÃO DE VEÍCULOS. Traz as diretrizes e os procedimentos para oferta e contratação de financiamento e arrendamento mercantil financeiro, especificamente para a aquisição de veículos. Cuida da regulamentação dos contratos de financiamento, da liberdade de escolha por parte dos clientes e de várias outras garantias legais previstas.

SARB nº 006/2009 — Sobre o MONITORAMENTO DE ADESÃO ÀS NORMAS DE AUTORREGULAÇÃO. Verifica sua aplicação efetiva e estabelece normas para a supervisão e o controle dos atos processuais definidos na autorregulação, sua comunicação e publicidade, além dos processos disciplinares e seus atenuantes, agravantes, etc.

SARB nº 007/2011 — Sobre os procedimentos relativos às demandas registradas no CANAL DE REGISTROS “CONTE AQUI”. Estabelece como são notificadas as signatárias e como são encaminhadas as solicitações de atendimento. Prevê como a ferramenta se articula com o canal governamental do Ministério da Justiça, o consumidor.gov.br.

SARB nº 008/2011 — Sobre as regras para o ENSINO ELETRÔNICO A DISTÂNCIA DA AUTORREGULAÇÃO. Trata de detalhar os mecanismos de gestão e aperfeiçoamento para ampliação da capacitação dos canais de e-learning. Cuida da regulamentação dos módulos de conteúdo, do público-alvo e das formas de avaliação do treinamento e seus prazos.

SARB nº 009/2013 — Sobre o PROGRAMA DE CERTIFICAÇÃO DE PROFISSIONAIS DE CRÉDITO IMOBILIÁRIO, DA ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DE CRÉDITO IMOBILIÁRIO E POUPANÇA (Abecip). Trata das normas, avaliação e classificação nos testes para certificação dos profissionais ligados ao importante setor do crédito imobiliário. Ressalta as condutas relativas ao próprio código de ética da FEBRABAN em sintonia com a certificação Abecip.

SARB nº 010/2013 — Sobre o CRÉDITO RESPONSÁVEL. Cuida de esclarecer os contextos sobre os limites de uso, a clareza dos conteúdos e a transparência dos contratos, da publicidade e demais informações colocadas à disposição dos contratantes, por meio físico ou virtual, na oferta das operações de crédito das instituições afiliadas.

SARB nº 011/2013 — Sobre a PREVENÇÃO E O COMBATE À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO. Trata da tipificação dos crimes e da apresentação das legislações e regulamentações disponíveis. Apresenta o “Conheça seu Cliente”, um conjunto de procedimentos para ajudar no rastreamento e identificação de recursos e clientes sob suspeição e no tratamento a pessoas expostas politicamente, entre outras garantias e medidas de segurança.

SARB nº 012/2014 — Sobre o RESUMO CONTRATUAL. Trata de definir as bases de todo o relacionamento das afiliadas com os consumidores que realizarem operações contratuais de crédito. Enfoca temas como a definição das margens de valores, tarifas, tributos, seguros, parcelas de pagamento, encargos, direitos do consumidor, etc.

SARB nº 013/2014 — Sobre a CONTRATAÇÃO DE CRÉDITO POR MEIOS REMOTOS. Especificamente para o crédito rotativo a pessoas físicas, trata das operações em canais como telefone, dispositivos móveis de comunicação, caixas eletrônicos de autoatendimento e internet. Discorre também sobre oferta, contratação, monitoramento das movimentações, desistência, etc.

SARB nº 014/2014 — Sobre a criação e implementação de políticas de RESPONSABILIDADE SOCIOAMBIENTAL. Cuida de expor os procedimentos legais fundamentais para a definição das ações ligadas à governança e às normas de sustentabilidade da Política de Responsabilidade Socioambiental (PRSA). Além disso, cuida dos termos das garantias imobiliárias e de crédito rural, entre outros temas afeitos ao setor.

SARB nº 015/2014 — Sobre o CRÉDITO CONSIGNADO. Trata das formas de oferta, contratação e operação, bem como das obrigações das instituições signatárias de oferecer alternativas como liquidação antecipada, direito de desistência, monitoramento, controle, etc.

SARB nº 016/2015 — Sobre a CONTA SALÁRIO. Fornece todas as informações essenciais para a sua abertura, condições de gratuidade, direitos do usuário, portabilidade, restrições, advertências quando do rompimento dos vínculos, encerramento da conta, etc.

SARB nº 017/2016 — Sobre a ADEQUAÇÃO DE PRODUTOS E SERVIÇOS. Visando à sustentabilidade e à harmonia das relações de consumo nas operações financeiras, a normativa prega uma adequação dos produtos e serviços oferecidos pelas instituições aos perfis específicos de seus clientes, assegurando qualidade, segurança e sustentabilidade.

SARB nº 018/2017 — Sobre o TRATAMENTO e a NEGOCIAÇÃO DE DÍVIDAS. Contribui para o resgate da capacidade financeira do consumidor nas contratações de crédito sem garantias, com o aperfeiçoamento da equidade, da boa-fé e da transparência. A concessão responsável do crédito, os canais de informação, negociação e de fechamento de acordos são também parte efetiva das normas de proteção e defesa do consumidor.

SARB nº 019/2018 — Sobre o USO CONSCIENTE DO CHEQUE ESPECIAL. Oferece orientações importantes para a consciência e a transparência no uso das condições e das informações do consumidor quanto à forma de parcelamento e liquidação do saldo devedor e outras garantias, visando à manutenção de uma relação de crédito saudável e sustentável.

SARB nº 020/2018 — Sobre os SELOS DE AUTORREGULAÇÃO. Expõe às signatárias os compromissos a serem firmados com a sociedade de forma que selos sejam concedidos às suas respectivas instituições em função dos níveis de adesão em que se encontrarem — signatária nível I, II ou III — e apresenta os procedimentos exigidos para a manutenção da qualificação.

SARB nº 021/2019 — Sobre o programa de integridade para PREVENÇÃO À CORRUPÇÃO E A ATOS LESIVOS À ADMINISTRAÇÃO PÚBLICA NACIONAL OU ESTRANGEIRA. Cuida de tipificar os procedimentos operacionais e os mecanismos de controle, rastreamento, denúncia de infrações e medidas disciplinares a serem observados pelas instituições financeiras signatárias. Trata desde a definição técnica do termo corrupção até os procedimentos de implantação, relacionamentos recomendáveis e preservação dos programas de integridade das afiliadas.

SARB nº 022/2019 — Sobre as OUVIDORIAS. Ressalta a necessidade de ampla divulgação dos canais de ouvidoria, incluindo os decretos oficiais do SAC. Prevê como se dá a gestão dos registros das demandas, os prazos para as respostas, a administração das pesquisas de satisfação e sua relação com os devidos planos de metas das afiliadas, além do constante aperfeiçoamento de sua capacitação.

SARB nº 023/2020 — Sobre o RELACIONAMENTO COM O CONSUMIDOR IDOSO. Visa a regulamentar a adequação dos produtos e serviços das instituições afiliadas a esse perfil de consumidor em particular. Prevê como adotar de forma legal os procedimentos do “Não Perturbe”, um conjunto de medidas de tratamento, educação, proteção contra abusos e diferenciação dos canais de atendimento ao idoso.

SARB nº 024/2020 – Sobre o RELACIONAMENTO COM OS CONSUMIDORES POTENCIALMENTE VULNERÁVEIS. Define o conceito de consumidor vulnerável e suas características, e a necessidade de se criar procedimentos para assegurar que a oferta de produtos e serviços sejam adequados a este público.

SARB nº 025/2020 – Sobre a PROTEÇÃO DE DADOS PESSOAIS. Estabelece diretrizes e procedimentos mínimos para aprimoramento da proteção de Dados Pessoais dos Titulares nos termos da LGPD e a necessidade de implementação de programa de governança em privacidade que estabeleça procedimentos mínimos e boas práticas para a adoção de medidas eficazes e capazes de demonstrar a observância e o efetivo cumprimento das normas de proteção de Dados Pessoais dos Titulares.

QUAIS SÃO OS EFEITOS DA AUTORREGULAÇÃO BANCÁRIA?

A adoção de uma regulamentação comum a todo o setor bancário resulta em uma maior transparência na relação entre os mais diversos parceiros da Instituição. Como as resoluções são continuamente atualizadas, os compromissos firmados estabelecem uma maior equidade concorrencial entre as instituições associadas ao padronizar as condutas de conformidade. A facilidade de consulta universal e democrática, partindo de uma mesma fonte na rede, é ferramenta importante para todos os colaboradores em todos os níveis de gestão e também uma garantia de informação sempre disponível a clientes, investidores, terceiros e a sociedade como um todo, possibilitando tanto o amplo acesso aos contextos e conteúdos de regulação, como a redução dos riscos de danos à imagem institucional por desconhecimento da matéria.

Para aprofundamento nas matérias aqui descritas, o Conglomerado CCB Brasil sugere abaixo, como leitura complementar importante, os documentos originais consultados na elaboração deste guia, os quais se encontram disponíveis para consulta pública. Confira:

Código de Autorregulação Bancária da FEBRABAN

SARB nº 001/2008
SARB nº 002/2008
SARB nº 003/2008
SARB nº 004/2009
SARB nº 005/2009
SARB nº 006/2009
SARB nº 007/2011
SARB nº 008/2011
SARB nº 009/2013
SARB nº 010/2013
SARB nº 011/2013
SARB nº 012/2014
SARB nº 013/2014
SARB nº 014/2014
SARB nº 015/2014
SARB nº 016/2015
SARB nº 017/2016
SARB nº 018/2017
SARB nº 019/2018
SARB nº 020/2018
SARB nº 021/2019
SARB nº 022/2019
SARB nº 023/2020
SARB nº 024/2021
SARB nº 025/2021

CÓDIGO DE ÉTICA E CONDUTA
http://www.br.ccb.com/menu/Institucional/Codigo-de-Etica-127

PLD
http://www.br.ccb.com/menu/Institucional/Governanca-Corporativa/Prevencao-a-Lavagem-de-Dinheiro%2C-a-Corrupcao-e-ao-Financiamento-ao-Terrorismo-188

FATCA/CRS
http://www.br.ccb.com/media/Institucional/guia-fatca-crs-ccb-brasil.pdf

6

Siglas

ABECIP — Associação Brasileira das Entidades de Crédito Imobiliário e Poupança

ANPD — Autoridade Nacional de Proteção de Dados

CCB — China Construction Bank

CCO — *Chief Compliance Officer*

CDE — Comitê da Diretoria Executiva

CEO — *Chief Executive Officer*

COAF — Conselho de Controle de Atividades Financeiras

CPPD — Comitê de Privacidade e Proteção de Dados

CRO — *Chief Risk Officer*

DPO — *Data Protection Officer*

FATCA/CRS — *Foreign Account Tax Compliance Act/Common Reporting Standard* ou Lei de Conformidade Tributária de Contas Estrangeiras/Modelo para Troca de Informações Tributárias

FCPA — *Foreign Corrupt Practices Act* ou

Lei Contra Práticas de Corrupção no Exterior

FEBRABAN — Federação Brasileira de Bancos

GAFI/FATF — Grupo de Ação Financeira/Financial Action Task Force

GTPPD — Grupo de Trabalho de Privacidade e Proteção de Dados

LGPD — Lei Geral de Proteção de Dados

OFAC — *Office of Foreign Assets Control* ou Agência de Controle de Ativos Estrangeiros dos Estados Unidos

ONU — Organização das Nações Unidas

PDA — *Personal Digital Assistant* ou Assitente Pessoal Digital

PLD — Prevenção à Lavagem de Dinheiro

PRSA — Política de Responsabilidade Socioambiental

RAS — *Risk Appetite Statement* ou Declaração de Apetite ao Risco

RIPD — Relatório de Impacto à Proteção de Dados

SAC – Serviço de Atendimento ao Consumidor

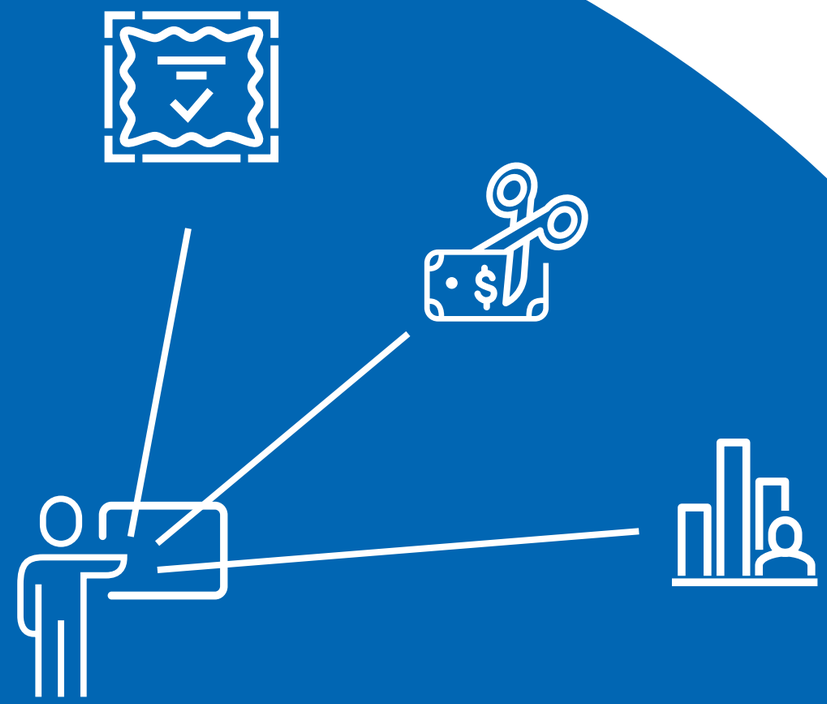
SARB — Sistema de Autorregulação Bancária

SDN — *Specially Designated Nationals and Blocked Persons List* ou Lista de Cidadãos com Designação Especial e Pessoas Suspensas

SI — Segurança da Informação

UE — União Europeia

UKBA — *United Kingdom Bribery Act* ou Lei Anticorrupção do Reino Unido



Ativo — Todo e qualquer bem tangível ou intangível pertencente, administrado ou de responsabilidade de uma instituição.

Ativo de informação — Todo e qualquer dado armazenado sob a posse e a responsabilidade de uma instituição. São informações estratégicas, arquivos, documentação de sistemas, manuais de procedimentos, planos de continuidade, treinamento, enfim, todo o suporte de negócios, toda a base da operação.

Ativos de software — Aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

Ativos físicos — Equipamentos computacionais (computadores, monitores, laptops, PDAs, pen drives, smartphones, tablets, modems, etc.), equipamentos de comunicação (roteadores, PABX, secretárias eletrônicas, telefones fixos ou celulares, etc.), mídias (fitas e discos magnéticos, discos óticos, disquetes, CDs, pen drives, etc.), outros equipamentos técnicos (no-breaks, aparelhos de ar condicionado, etc.), mobiliários e suas acomodações.

Autorregulação — Conjunto de normas e preceitos técnicos voluntariamente estabelecidos em conjunto por instituições de um determinado setor para o monitoramento, a fiscalização e a criação de referenciais éticos e práticas comuns. É estruturada a partir da criação, negociação e constante atualização de documentos aceitos e firmados por todos as partes reguladas.

Colocação — Ingresso no sistema financeiro de recursos provenientes de atividades ilícitas, por meio de depósitos, compra de instrumentos financeiros (ex.: CDBs, quotas de fundos, etc.) ou compra de bens ou ativos.

Comitê de Controles Internos — Comitê que tem por objetivo assessorar o Comitê de Diretoria Executiva (CDE) no desempenho de suas atribuições relacionadas à adoção de políticas e medidas voltadas à disseminação da cultura de controles internos, identificação, mitigação de riscos e conformidade com normas aplicáveis à Instituição.

Compliance — É o dever de cumprir, de estar em conformidade com leis, diretrizes, regulamentos internos e externos, e fazer com que sejam cumpridos, buscando mitigar o risco atrelado à reputação e o risco legal ou regulatório.

Conduta — Manifestação do modo como uma pessoa ou instituição se comporta perante a sociedade, tendo como base a lei, as crenças, os valores morais e éticos que seguem e preconizam.

Confidencialidade — Garantia de que uma determinada informação somente será acessada por pessoas efetivamente autorizadas.

Conflito de interesses — Qualquer situação na qual uma pessoa ou instituição possa ter sua capacidade de julgamento e decisão afetada, podendo incorrer na quebra do princípio de imparcialidade e favorecer interesses próprios, de terceiros ou, ainda, de cunho político ou ideológico, em detrimento dos interesses e princípios da comunidade em que está inserida.

Conselho de Administração — É uma das formas de gestão comuns às boas práticas de governança corporativa e consiste no estabelecimento de uma estrutura organizacional que concilie interesses e alinhe estratégias de forma transparente e autônoma. É também chamado comumente de board e é a ele que os CEOs se reportam para comunicar ações e prestar esclarecimentos.

Corrupção — No sentido jurídico geral do termo, é um crime cometido por funcionários de administrações públicas ou privadas que se caracteriza pela conduta de forma a oferecer ou obter vantagens ilegais ou favores indevidos em troca de ganhos ilícitos. Pode ser ativa ou passiva, interna ou externa, e os tipos mais comuns são o suborno, propina, nepotismo, extorsão, tráfico de influência, utilização de informação privilegiada para fins pessoais ou de pessoas amigas ou parentes, compra e venda de sentenças judiciárias, recebimento de presentes ou de serviços de alto valor, improbidade, peculato, fraude, conluio e prevaricação. A corrupção penetra em diversos setores da sociedade, compromete uma porção importante dos recursos do Estado e ameaça a estabilidade política e o

desenvolvimento sustentável de uma nação. A corrupção afeta a transparência e é uma ameaça ao equilíbrio, segurança e sobrevivência das sociedades, enfraquecendo as instituições e os valores da democracia, da ética e da justiça e comprometendo o desenvolvimento sustentável.

Disponibilidade — Prerrogativa de usuários autorizados a obter acesso à informação e aos sistemas correspondentes sempre que necessário, nos períodos e ambientes aprovados pela Instituição.

Ética — Conjunto de princípios e valores que norteiam a boa conduta de um ser humano de forma geral. É diferente de moral, que se baseia em aspectos de comportamento segundo visões particulares, específicas.

FCPA — O Foreign Corrupt Practices Act é a Lei contra Práticas de Corrupção no Exterior promulgada pelo Congresso dos EUA em 1977 e destinada a criar sanções cíveis, administrativas e penais no combate à corrupção comercial internacional. Essa lei se aplica a pessoas físicas e empresas norte-americanas que, em atividade comercial no exterior, utilizem-se de corrupção no poder público estrangeiro para obter ou reter transações comerciais no país em questão.

Head Office — Em tradução direta, é o Escritório Central, mas refere-se, no campo empresarial, à sede da empresa, onde se situam seus principais gestores. Também pode ser referida como Corporate Headquarters.

Informação — É um ativo que registra dados de clientes, dados de negócios, configurações de sistemas, entre outros, e que, portanto, deve ser classificado conforme seu valor para a organização e, a partir dessa classificação, ser adequadamente protegido nos aspectos de confidencialidade, integridade e disponibilidade. A informação pode ser registrada de diversas formas, por exemplo, impressa ou escrita em papel, armazenada em computadores, disquetes, CDs ou outras mídias, transmitida pelo correio ou por meios eletrônicos, exibida em filmes ou falada em conversas.

Instituição financeira — Pessoa jurídica de direito público ou privado, conforme a Lei nº 7.492/86, que tenha como atividade principal ou acessória, cumulativamente ou não, a captação, intermediação ou aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira, ou a custódia, emissão, distribuição, negociação, intermediação ou administração de valores mobiliários.

Integração ou reintegração — Retorno ao sistema econômico dos recursos ilícitos advindos de modo aparentemente lícito, mediante investimento no mercado de capitais (ex.: ações, títulos e valores mobiliários), mercado imobiliário, joias, empresas produtivas, turismo, obras de arte, fundos mútuos, etc.

Integridade — Garantia de que a informação somente será modificada por pessoas efetivamente autorizadas a fazê-lo, sempre dentro dos métodos aprovados para tal.

Lavagem de dinheiro — Prática utilizada para encobrir a origem ilegal de um recurso financeiro. É o processo em que os ganhos "sujos", originados de atividades ilícitas, tornam-se "limpos" ou aparentemente legalizados após operações diversas que envolvem, teoricamente, quatro fases independentes, que, com frequência, ocorrem simultaneamente: colocação, ocultação, integração ou reintegração, e reciclagem.

Ocultação — Execução de uma ou múltiplas operações financeiras com os recursos já ingressados no sistema financeiro, objetivando a ocultação dos recursos ilegais, os quais efetivamente se misturam àqueles de origem lícita.

Reciclagem — Limpeza completa dos rastros do crime financeiro, encerrando contas bancárias, sacando valores, simulando venda de bens. O combate a essa prática é de extrema importância uma vez que as consequências sociais desse crime são destruidoras, pois prejudicam a economia formal, acarretando danos ao sistema financeiro e diminuição dos investimentos públicos em benefício da sociedade, como saúde, segurança e educação, entre outros.

Signatária — Toda e qualquer pessoa ou instituição associada a um grupo determinado cujos princípios, valores e atitudes tenham sido previamente estabelecidos em um acordo de compromisso assinado.

Signatárias FEBRABAN nível I — Instituições financeiras signatárias ao Código de Conduta Ética e Autorregulação da FEBRABAN.

Signatárias FEBRABAN nível II — Instituições financeiras signatárias que aderiram a pelo menos um dos eixos normativos do SARB.

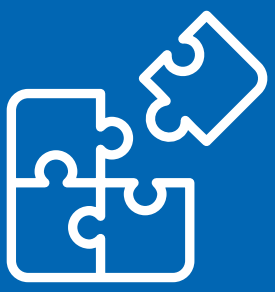
Signatárias FEBRABAN nível III — Instituições financeiras signatárias que aderiram a todos os eixos normativos do SARB.

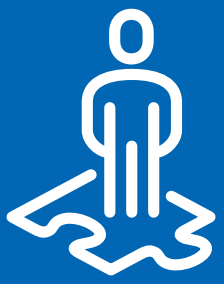
Segurança da informação — Preservação da confidencialidade, disponibilidade e integridade das informações, conforme definido pela norma NBR ISO/IEC 27002.

Stakeholder — As partes interessadas, os chamados grupos de interesse. São os parceiros de todos os segmentos da sociedade que normalmente estão de acordo com as práticas de governança corporativa executadas pelas instituições ou que façam parte de sua definição.

Terrorismo — Uso sistemático do terror ou da violência imprevisível contra regimes políticos, povos ou pessoas para alcançar um fim político, ideológico ou religioso. Os recursos utilizados no financiamento do terrorismo não são necessariamente originários de atividades criminosas, prerrogativa da maioria dos crimes de lavagem de dinheiro. A organização, a manutenção e o desenvolvimento operacional de redes terroristas pressupõem uma atividade em contínua evolução e, paralelamente, a procura constante de métodos novos e intermutáveis de obtenção de fundos e de sua movimentação através de canais legais e ilegais, entre os quais se encontram as sociedades comerciais internacionais, os trusts e empresas offshore, os corretores de valores, a transferência de fundos através do sistema “hawala” (por meio de doleiros) ou a utilização de associações de beneficência. As instituições financeiras desempenham um papel fundamental na prevenção e no combate aos atos ilícitos. Sendo o grande desafio identificar e reprimir operações cada vez mais sofisticadas, as políticas de prevenção à lavagem de dinheiro, à corrupção e ao financiamento ao terrorismo adotadas pelo conglomerado CCB Brasil encontram-se em conformidade com as legislações, normas e regulamentações complementares vigentes.

UKBA — United Kingdom Bribery Act ou Lei Anticorrupção do Reino Unido. Entrou em vigor em 1º de julho de 2011 e é considerada uma das leis de combate à corrupção mais rígidas do mundo, punindo, inclusive, a corrupção privada. Assim como as principais leis anticorrupção existentes, ela também possui a chamada extraterritorialidade, sendo aplicável não apenas às empresas britânicas que operam no mercado local e/ou em mercados estrangeiros, mas também às sociedades estrangeiras que atuam no Reino Unido. Prevê ainda a punição de pessoas físicas e jurídicas pelo cometimento de qualquer dos crimes contidos no texto legal.





CCB 中国建设银行
China Construction Bank