POLÍTICA DE CONTROLE INTERNO, RISCOS E COMPLIANCE DO CERUS BANK

1. INTRODUÇÃO

O termo *compliance* origina-se do verbo inglês "*to comply*", que tem como significado: cumprir, obedecer, executar e satisfazer aquilo que lhe foi imposto (definido). Desta forma, *compliance* é o dever de estar em conformidade, fazer cumprir e cumprir as leis, regulamentos internos e externos, processos, procedimentos, políticas e diretrizes, visando à mitigação do risco legal e dos riscos relacionados à reputação.

O Cerus Bank, em conformidade com as resoluções e circulares expedidas pelo Banco Central do Brasil (BACEN), apresenta esta Política de Controles Internos & *Compliance* ("Política"), elaborada de acordo com as normas vigentes e as boas práticas de mercado. Complementarmente a esta Política, deve ser também observado e respeitado o Código de Ética e Conduta do Cerus Bank.

2. OBJETIVO

A presente Política tem a função de firmar as regras, procedimentos e mecanismos que assegurem e viabilizem o permanente atendimento às normas e regulamentações vigentes referentes à própria atividade de gestão de recursos de terceiros, valores mobiliários e fundos de investimentos e aos padrões éticos e profissionais aplicáveis.

3. PROCESSO DE *COMPLIANCE*

A área de *Compliance* tem a responsabilidade de monitorar, implementar, rever e estimular os sistemas de controles internos no Cerus Bank, com o objetivo de assegurar que as atividades estão sendo cumpridas e executadas em conformidade com as regras e controles internos e órgãos reguladores e autorreguladores, por meio da disseminação de elevados padrões éticos e de integridade. Deve-se enfatizar a importância dos controles internos e o papel de cada um nos processos da instituição.

O processo de *compliance* é segmentado em quatro etapas: *(a) identificação; (b) análise; (c) tratamento e (d) monitoramento e revisão.*

a. Identificação

O risco de *compliance* refere-se ao risco legal de sanções regulatórias, de perda financeira ou perda de reputação, resultantes de falhas nos cumprimentos de leis, códigos de conduta, regulamentações, autorregulamentações, políticas e procedimentos internos e boas práticas que englobam matérias como gerenciamento de segregação de função, conflitos de interesses, princípios éticos, entre outros.

b. Análise

A responsabilidade direta pelas atividades relacionadas a controles internos e *compliance* e, consequentemente, a esta Política, é atribuição do Gerente de Gestão de Riscos & *Compliance*.

Funções do Responsável por *Compliance*

- acompanhar e atualizar os códigos, diretrizes, políticas, procedimentos e controles internos;
- certificar a aderência e cumprimento das leis, regulamentações, instruções e normas emitidas pelos órgãos reguladores e autorreguladores, relativas à atividade de gestão de recursos de terceiros, valores mobiliários e fundos de investimentos, assim como suas atualizações;
- assegurar a adequação dos integrantes do Cerus Bank aos códigos, diretrizes, políticas, procedimentos, processos e controles internos;
- garantir que o relacionamento entre integrantes, sócios, clientes, concorrentes, fornecedores e prestadores de serviço esteja sendo realizado em conformidade com as leis, regulamentações, instruções e normas emitidas pelos órgãos reguladores e autorreguladores e com as políticas e procedimentos do Cerus Bank;
- levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática em desacordo com as disposições desta Política e das demais normas aplicáveis à atividade do Cerus Bank para apreciação do Comitê de *Compliance*;
- assegurar a adequada segregação de atividades a fim de evitar conflitos de interesse;
- identificar possíveis condutas contrárias a esta Política;
- assessorar o gerenciamento dos negócios no que se refere à interpretação e impacto da legislação, monitorando as melhores práticas em sua execução e analisar, periodicamente, as normatizações emitidas pelos órgãos normativos, como o BACEN e outros organismos congêneres e acionar e conscientizar as áreas responsáveis pelo cumprimento, atuando como facilitador e incentivador do entendimento das mesmas;
- convocar e organizar as reuniões do Comitê de *Compliance*, ou com os demais integrantes, sempre que julgar necessário;
- preservar a identidade de integrantes que reportem qualquer conduta ilegal, antiética ou contrária a esta Política ou aos códigos, diretrizes, políticas, procedimentos, processos e controles internos e garantir que os mesmos não sofrerão consequências negativas devido ao comunicado; e
- disseminar a cultura de controles internos e *compliance* para assegurar o cumprimento de leis e regulamentos existentes.

Comitê de *Compliance*

- definir os princípios éticos a serem observados por todos os integrantes do Cerus Bank, constantes nesta Política, nas leis e normas emitidas pelos órgãos reguladores e autorreguladores ou nas políticas e procedimentos internos do Cerus Bank;
- promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os integrantes do Cerus Bank, inclusive por meio de treinamentos;
- apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos de *compliance* previstos nesta Política ou nos códigos, diretrizes, políticas, procedimentos, processos e controles internos do Cerus Bank, e também apreciar e analisar situações não previstas;
- garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
- solicitar sempre que julgar necessário, para a análise de suas questões, visando à perfeita aplicação desta Política, bem como, ao perfeito atendimento das leis e normas aplicáveis ao Cerus Bank, o apoio da auditoria interna ou externa ou outra assessoria;
- tratar todos os assuntos que cheguem ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa do Cerus Bank, como também dos envolvidos;
- definir eventuais penalidades a integrantes, quando julgar necessário;
- analisar situações que possam ser caracterizadas como “conflitos de interesse” pessoais e profissionais, inclusive, mas não limitadamente, em situações que envolvam:
    - investimentos pessoais;
    - transações financeiras com clientes fora do âmbito do Cerus Bank;
    - recebimento de favores ou presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;
    - análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o integrante possua alguma relação pessoal;
    - análise financeira ou operação com empresas em que o integrante possua investimento próprio;
    - participações em alguma atividade política; ou participação em funções e atividades externas.

c. Tratamento

Segregação de Atividades

O Cerus Bank atua como Instituição de Pagamento (IP), um arranjo de pagamento que, possibilita aos seus clientes realizar movimentações financeiras, pagamentos e contrair empréstimos em instituições financeiras parceiras devidamente conveniadas, dentre outros serviços. As atividades desempenhadas pelo Cerus Bank são reguladas pela Banco Central do Brasil (BACEN).

Neste sentido, quando necessário, deve ser assegurado aos integrantes, clientes e às autoridades reguladoras e autorreguladoras, a completa segregação de suas atividades, adotando procedimentos operacionais objetivando a segregação e evitando possíveis situações de conflito. Adicionalmente, todos os integrantes do Cerus Bank devem trabalhar para que suas funções e atividades estejam alinhadas às suas responsabilidades evitando, ao máximo, situações que possam resultar em conflitos de interesses.

Conflito de Interesses

Um conflito de interesses inclui qualquer situação na qual um integrante esteja envolvido em duas ou mais atividades ou relacionamentos que, em algum grau, são incompatíveis. Nestas situações suas atividades ou conduta podem conflitar com a sua função no Cerus Bank, ou podem afetar o seu julgamento e desempenho. Ademais, o conflito de interesse pode surgir em situações decorrentes do desempenho de funções de determinado integrante nas quais os interesses pessoais de tal integrante possam ser divergentes ou conflitantes com os interesses do Cerus Bank e/ou de seus clientes.

Todo integrante do Cerus Bank deve avaliar, antes de se comprometer em qualquer atividade ou função, ou mesmo participar em operação ou relacionamento, se esta ação pode acarretar um conflito. Integrantes do Cerus Bank tem o dever de agir com boa-fé e de acordo com os interesses dos clientes e da companhia, com o intuito de não ferir a relação fiduciária com eles.

Neste contexto, os integrantes ficam proibidos de exercer atividades profissionais externas ao Cerus Bank, remuneradas ou não, salvo se previamente aprovadas pelo Comitê de *Compliance*, respeitando sempre que:

- é proibida qualquer atividade ilícita;
- é vetado ao integrante trabalhar para qualquer concorrente da Companhia ou atuar como diretor, representante ou consultor da mesma; e
- é vedada a condução de atividades paralelas, inclusive filantrópicas e civis, durante a jornada de trabalho, ou que de qualquer forma afetem o desempenho do integrante durante a jornada de trabalho.

Adicionalmente, o responsável por *Compliance* deve fazer parte do Comitê de Remuneração do Cerus Bank com o intuito de monitorar e participar da formulação das políticas de incentivos da Companhia, de maneira a assegurar que (i) a política de remuneração do Cerus Bank não leve a conflitos com os interesses de clientes e (ii) taxas, comissões e encargos pagos a terceiros ou recebidos de terceiros não levem a conflitos com os interesses dos clientes.

Know Your Client

O Cerus Bank adota a política de análise e identificação do cliente com o objetivo de conhecê-los, estabelecendo um conjunto de regras que propiciem identificar e conhecer a origem e constituição do patrimônio e dos recursos financeiros do cliente. Os integrantes devem cadastrar os clientes do Cerus Bank previamente ao início da atividade de gestão de recursos. O cadastramento deve ser feito de acordo com os procedimentos estabelecidos pelos normativos do BACEN, sendo validado e atualizado periodicamente.

Adicionalmente, o Cerus Bank conta com os esforços de todos os colaboradores e prestadores de serviços para:

(i) realizar a identificação de clientes novos ou já existentes, e promover sua atualização com periodicidade; e
(ii) prevenir, detectar e reportar quaisquer operações suspeitas.

Nesse sentido, o responsável por *Compliance* deve acompanhar as atividades dos setores integrantes do Cerus Bank.

Além disso, o Cerus Bank, com o acompanhamento do responsável por *Compliance*, deverão estabelecer uma análise independente e assegurar um processo reforçado de *due diligence* com relação às Pessoas Politicamente Expostas (“PEP”), definidas como pessoas que exerceram altos cargos de natureza política ou pública, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

d. Monitoramento e revisão

A partir do monitoramento, avaliações e acompanhamento diário das atividades do Cerus Bank, o responsável por *Compliance* deve identificar as deficiências e não conformidades a fim de implementar ações corretivas. Adicionalmente, é atribuição do responsável por *Compliance* a comunicação das não conformidades e deficiências identificadas para o Comitê de *Compliance*.

Os integrantes do Cerus Bank que identificarem qualquer situação que possa afetar, de maneira negativa, as atividades e a reputação da organização devem informar ao responsável por *Compliance*, imediatamente, resguardados pela segurança e preservação de sua identidade e o não sofrimento de consequências negativas em detrimento desta atitude.

Visto que a área de *Compliance* tem por objetivo ajudar a organização e seus integrantes a se adequarem às determinações dos reguladores e aos códigos, diretrizes, políticas e procedimentos internas, cabe a qualquer integrante do Cerus Bank informar ao responsável por *Compliance*, de maneira justa, honesta e respeitosa, sobre a ocorrência de qualquer conduta ilegal, antiética ou contrária a leis e normas emitidas pelos órgãos reguladores e autorreguladores ou às normas internas da instituição por parte de qualquer integrante da organização.

4. CONFIDENCIALIDADE

Frequentemente, os integrantes do Cerus Bank serão expostos a informações confidenciais relacionadas ao negócio, que incluem, além de informações a respeito da própria instituição (Cerus Bank), informações e assuntos relacionados aos seus clientes, parceiros comerciais e fornecedores, e informações relativas aos demais integrantes.

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada fora do ambiente do Cerus Bank, fornecida ao público, mídia ou a demais órgãos, sem a devida autorização do Comitê de Compliance. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais, Código de Ética e Conduta do Cerus Bank e esta Política.

São consideradas informações confidenciais, por exemplo:

- processos, metodologias, modelos, sistemas do Cerus Bank e parceiro(a)s;
- informações técnicas, informações financeiras, informações comerciais; e
- estratégias de aberturas de contas, gestão de investimento, política de crédito, saldos, extratos, posições de clientes, operações estruturadas e demais operações e seus respectivos valores, estruturas, programas de ação, relacionamentos com clientes, contrapartes comerciais, fornecedores e prestadores de serviços, informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades do Cerus Bank e a seus sócios e clientes.

Princípios a serem observados pelos integrantes ao lidarem com informações:

- todas as informações devem ser consideradas confidenciais, seja em formato escrito, verbal ou eletrônico / digital;

- informações pessoais a respeito de indivíduos devem ser tratadas como sendo confidenciais;
- comentar ou fornecer informações relacionadas ao negócio do Cerus Bank somente se fizer parte da função do integrante ou com autorização; e em situação de dúvida, consultar o responsável pela área *Compliance*.

Visando à proteção de informações confidenciais ao utilizar meios eletrônicos de comunicação, deve-se adotar extrema cautela em relação aos riscos associados a tal prática. Na questão de confidencialidade e tratamento da informação, o integrante deve ainda considerar a seguinte situação:

Informação privilegiada: considera-se informação privilegiada uma informação relevante e material a respeito de qualquer companhia, produto e/ou serviço, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas parceiras ou investidas ou com terceiros). As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

5. COMBATE E PREVENÇÃO À LAVAGEM DE DINHEIRO

Entende-se por lavagem de dinheiro práticas econômico-financeiras que têm por finalidade dissimular a origem ilícita de determinados ativos, de forma que os mesmos aparentem ter origem lícita. Qualquer suspeita de operações financeiras e não financeiras que possam apresentar indícios ou evidências de envolverem atividades relacionadas aos crimes de lavagem de dinheiro devem ser comunicadas imediatamente ao responsável por *Compliance* do Cerus Bank.

Consideram-se atividades suspeitas:

- as que podem estar relacionadas com recursos provenientes de atividades criminosas ou tenham como objetivo ocultar recursos ou ativos com tal origem;
- as que possam comprometer recursos que, direta ou indiretamente, serão utilizados, no todo ou em parte, para a prática de atividades de natureza terrorista;
- as que estejam fracionadas ou estruturadas para evitar alguns dos registros ou comunicações sistemáticas em virtude da legislação aplicável contra a lavagem de dinheiro e o financiamento do terrorismo;
- as que não tenham uma finalidade comercial ou em relação àquelas para as quais não exista uma explicação razoável, após examinados os fatos conhecidos, incluídos no histórico e o possível objetivo das operações;

– as que envolvam montantes cujos valores sejam incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial/financeira de qualquer das partes envolvidas, tomando-se por base as informações cadastrais respectivas.

O responsável por *Compliance* juntamente com o Comitê de *Compliance* analisará e conduzirá o caso às autoridades competentes. A análise será feita caso a caso, mediante avaliação dos instrumentos utilizados, a forma de realização, as partes e valores envolvidos, a capacidade financeira e a atividade econômica dos envolvidos e qualquer indicativo de irregularidade ou ilegalidade a operação. O Cerus Bank compromete-se a comunicar ao COAF (Conselho de Controle de Atividades Financeiras – Coaf) todas as transações ou propostas que possam constituir indícios de crimes de "lavagem" ou ocultação de bens, direitos e valores provenientes de crimes elencados na legislação aplicável.

O responsável por *Compliance* deve emitir relatório com periodicidade anual listando as operações identificadas como suspeitas, e as operações ou propostas de operações devidamente comunicadas às autoridades competentes que, na forma da legislação vigente, caracterizam indício de lavagem de dinheiro. Os processos de registro, análise e comunicação, às autoridades competentes, de operações financeiras que revelam indício de lavagem de dinheiro são realizados de forma sigilosa, inclusive em relação aos envolvidos.

No caso de envolvimento de integrantes em operações dessa natureza, ficarão sujeitos às penalidades previstas nesta Política. Além das consequências legais cabíveis, o integrante estará sujeito a desligamento ou exclusão por justa causa, caso o integrante que seja sócio do Cerus Bank, ou demissão por justa causa, caso o integrante seja empregado do Cerus Bank, ou ainda, ou rescisão de contrato se prestador de serviços junto a instituição.

Cabe ao responsável por *Compliance*:

- monitorar e fiscalizar periodicamente o cumprimento, pelos integrantes, o combate e prevenção à lavagem de dinheiro;
- fiscalizar os procedimentos contra lavagem de dinheiro;
- definir políticas, procedimentos e treinamentos de *compliance* para assegurar o cumprimento das regras contra lavagem de dinheiro;
- acompanhar o desenvolvimento e implementação nas áreas de negócios de ferramentas de controle, tais como cadastro de clientes, *know your client* e renovação de cadastro periodicamente; e
- acompanhar o desenvolvimento e implementação nas áreas de negócios de sistemas de monitoramento com critérios pré-estabelecidos (como limites e movimentações) e monitoramento da área de contas a pagar e contas a receber.

6. COMBATE À CORRUPÇÃO

A Lei Anticorrupção (nº 12.846/13) Brasileira, vigente desde 01 de agosto de 2013, e seu respectivo Decreto Regulamentar 8.420, de 18 de março de 2015, dispõem sobre a responsabilidade civil e administrativa de sociedades brasileiras ou estrangeiras que atuem no Brasil por conta de atos de seus diretores, gerentes, funcionários e outros agentes que atuem em nome da sociedade que envolvam a prática de corrupção contra a administração pública, nacional ou estrangeira, inclusive organizações públicas internacionais, como suborno e fraude em licitações e contratos administrativos da administração pública.

Nos termos das normas acima mencionadas, suborno significa prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada, incluindo os chamados “pagamentos facilitadores”. Complementando, entende-se por corrupção qualquer ato ou efeito de se corromper, oferecer algo para obter vantagem onde se favorece uma pessoa e se prejudica outra. Inclui-se aqui os atos ilegais caracterizados por falsidade, encobrimento ou violação da confiança, cometido por um indivíduo ou organização para: obter dinheiro, propriedade ou serviços, evitar pagamento ou perda de serviços ou garantir vantagem pessoal ou profissional.

Os integrantes do Cerus Bank, sempre que perceberem algum ato com suspeita ou confirmação de corrupção, devem comunicar imediatamente ao responsável por *Compliance*. Os atos podem envolver parceiros externos, clientes ou potenciais clientes.

7. SEGURANÇA, SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICOS

As medidas de segurança, segurança da informação e segurança cibernética têm por finalidade minimizar as ameaças aos negócios e atividades do Cerus Bank, ao sigilo de dados de seus colaboradores, clientes e fornecedores, assim como garantir a integridade funcional do parque tecnológico da Companhia.

As políticas, métodos e procedimentos adotados pelo Cerus Bank visam refletir as melhores práticas de mercado, levando em consideração o porte e a sensibilidade a riscos que está exposta a organização. Em conformidade com o Guia de Ciber segurança Anbima de Dez/2017, organizamos esta seção em cinco funções: identificação e avaliação de riscos; ações de prevenção e proteção; monitoramento e testes; criação do plano de resposta; e reciclagem e revisão. Tendo assim um documento específico apenas para este item.

8. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

O Cerus Bank busca como boa prática dentro de seu segmento de atuação, manter-se atualizado com os avanços tecnológicos que propiciam aumento de produtividade na condução de suas atividades. Ao mesmo tempo em que a adoção de tais tecnologias é benéfica aos clientes da companhia, já que propiciam um serviço de melhor qualidade para os mesmos, a implementação de novos sistemas, softwares e hardwares expõe a Companhia e seus clientes a riscos potenciais.

Com base no modelo de negócios atual do Cerus Bank, e levando em consideração o porte da Companhia e os mercados em que a mesma atua, é possível mapear as seguintes motivações que poderiam fazer com que a Companhia viesse a ser alvo de ataques mal-intencionados:

- Obter ganho financeiro;
- Roubar, manipular ou adulterar informações;
- Obter vantagens competitivas e informações confidenciais de empresas concorrentes.
- Fraudar, sabotar ou expor a instituição invadida, por razões diversas;

A área mais sujeita a ataques, neste caso, é a de dados e informações tanto de uso interno do Cerus Bank quanto de seus clientes e empresas parceiras. As informações relevantes utilizadas na condução dos negócios da Companhia são classificadas como: informações de ativo (patrimônio, investimentos, políticas internas, entre outros); informações de passivo (dados de cotistas, histórico de patrimônio e movimentações, entre outros); estratégicas (projetos sob avaliação, estudos em desenvolvimento, entre outros); operacionais (senhas, tokens, nome de usuário, entre outros); e informações de domínio público (dados históricos já divulgados, materiais obtidos via internet, entre outros).

A classificação de informações permite mapear os riscos a que a F3 se encontra mais exposta, e priorizar a segurança de dados e informações críticos. Os métodos mais prováveis de ataque cibernético, e, portanto, acompanhados pela Companhia, são *Malwares* e engenharia social. Outra possível fonte de possível risco acompanhada pela Companhia são falhas operacionais que podem resultar na divulgação de dados sigilosos sem intenção explícita.

O Cerus Bank leva em consideração também que a instituição está exposta a riscos de segurança físicos, que devem ser tratados de maneira a garantir a integralidade e continuidade de seus negócios, assim como zelar pelo bem-estar de seus colaboradores.

9. AÇÕES DE PREVENÇÃO E PROTEÇÃO

As instalações do Cerus Bank são protegidas por controles de entrada apropriados para assegurar a segurança dos integrantes e proteger as instalações e bens do Cerus Bank, além do sigilo, integridade e disponibilidade de qualquer informação ou bem da instituição.

O acesso de terceiros às dependências do Cerus Bank somente é permitido com a permissão expressa de um integrante do Cerus Bank e acompanhado do mesmo. Adicionalmente, o acesso físico de terceiros às áreas em que servidores, informações confidenciais ou proprietárias possam estar presentes ou possam estar sendo discutidas deve ser limitado e restrito. O acesso a estas áreas deve ocorrer somente com autorização do responsável por Compliance, ou do responsável pelo respectivo setor / departamento. Quaisquer discussões específicas relativas ao Cerus Bank, clientes ou projetos confidenciais deverão se restringir e ocorrer em áreas restritas e seguras.

A rede da organização é protegida por firewall, sendo que cada máquina individualmente possui proteção redundante de firewall, assim como softwares de proteção contra *Malwares*. Todos os equipamentos da rede do Cerus Bank estão acomodados em um espaço fechado e isolado. Adicionalmente, todos as informações e serviços críticos as operações do Cerus Bank, como bancos de dados e sistemas, estão hospedados em servidores externos ao Cerus Bank (cloud service), cujos acessos são de exclusividade, única e tão somente, dos sócios-diretores e de responsáveis previamente autorizados.

Todas as estações de trabalho do Cerus Bank são fixas e com computadores / Notebooks seguros. No caso de o integrante ficar afastado por longos períodos da estação de trabalho, como no horário de almoço, as sessões abertas devem ser trancadas e documentos sensíveis deverão ser retirados da mesa e armazenados em gavetas ou armários. Ao final do expediente de trabalho o integrante deve organizar sua mesa e guardar todos os papéis e dispositivos de armazenamento.

É terminantemente proibido que os integrantes façam cópias (físicas ou eletrônicas) de arquivos utilizados, gerados ou disponíveis na rede do Cerus Bank, e circulem estes arquivos em ambientes externos à instituição, sem objetivo relacionado às suas atividades e funções na organização e sem autorização prévia. Neste sentido, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora.

O Cerus Bank não mantém arquivo físico centralizado, sendo cada integrante responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo. O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

O Cerus Bank possui e mantém uma Política de Mesa Limpa para estabelecer uma cultura de segurança e confiança para todos os integrantes do Cerus Bank e proteger documentos que contenham informações confidenciais sobre nossos clientes e fornecedores em suas estações de trabalho, impressoras e salas de reunião.

Fica proibida a conexão de equipamentos externos (pendrives, hd externos, etc) na rede Cerus Bank que não tenham vinculação com a função ou atividade do integrante e não estejam previamente autorizados pelo responsável do respectivo setor. A utilização dos ativos e sistemas do Cerus Bank, incluindo computadores / notebooks, telefones / celulares, internet, e-mail e demais aparelhos se destina exclusivamente a fins profissionais. O uso indiscriminado dos mesmos para fins pessoais deve ser evitado.

Os e-mails do Cerus Bank caracterizam-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização voltada para alcançar os fins comerciais do Cerus Bank. O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação do Cerus Bank. O recebimento de e-mails muitas vezes não depende do próprio integrante, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o integrante deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores / notebooks do Cerus Bank.

A visualização de sites, blogs, fotologs, webmails, redes socais, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida. A senha e login para acesso aos dados contidos em todos os computadores / notebooks, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador (integrante) e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. Dessa forma, o integrante poderá ser responsabilizado caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

Cada integrante é responsável, ainda, por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Todo integrante deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum integrante identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar ao responsável por Compliance.

Os computadores e arquivos de e-mails corporativos poderão ser inspecionados pelo Cerus Bank, por meio do responsável por Compliance, a qualquer tempo e independentemente de prévia notificação para a verificação da observância do disposto na presente Política, ou nas demais hipóteses previstas nesta Política e Código de Ética e Conduta.

Considerando que a utilização de computadores / notebooks, telefones / celulares, internet, e-mail e demais equipamentos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das funções e atividades dos integrantes, o Cerus Bank reserva-se ao direito de monitorar a utilização de tais meios.

10. MONITORAMENTO E TESTES

A área de tecnologia da informação (TI) efetuará verificações semestrais na rede corporativa, para validar o acesso seguro aos recursos disponíveis. As irregularidades encontradas durante essas verificações devem ser comunicadas ao responsável por *Compliance*. O bloqueio de acesso à rede do Cerus Bank poderá ser efetuado pelo responsável de TI sempre que solicitado e aprovado pelo Comitê de *Compliance*, ou caso seja detectado algum risco para a rede ou para os sistemas da instituição.

A área de TI também poderá verificar periodicamente as informações armazenadas nos dispositivos de armazenamento, estejam eles nos servidores ou nas estações de trabalho, para garantir o armazenamento apenas das informações que sejam realmente vinculadas ao Cerus Bank ou à função do respectivo integrante.

11. CRIAÇÃO DO PLANO DE RESPOSTA

Em casos de concretização de falhas de segurança, como vazamento de informações críticas, o Comitê de Riscos e *Compliance* deverá se reunir de forma a elaborar um plano de contingência emergencial para lidar com as consequências da falha específica, que podem variar de acordo com o tipo de falha. O plano de respostas deverá abranger ações imediatas para tentar minimizar os impactos do ocorrido, assim como, em um segundo momento, propor melhorias nas ações preventivas, e identificar e punir, conforme o caso, colaboradores envolvidos.

12. RECICLAGEM

A Política de Segurança, Segurança da Informação e Segurança Cibernética do Cerus Bank deverá ser revisada, no mínimo, anualmente, de forma a analisar evoluções no parque e no ambiente tecnológico em que está inserida a instituição. Esta atualização, conduzida em conjunto com a revisão da presente Política, tem o propósito final de adaptar e melhorar os procedimentos aqui delineados, aumentando a segurança e resiliência organizacional do Cerus Bank.

13. PLANO DE CONTINUIDADE DE NEGÓCIOS

O objetivo do Plano de Continuidade de Negócios do Cerus Bank é estabelecer as medidas e estrutura do plano de resposta a ser adotado em momentos de crise que acarretem, ou possam vir acarretar, em descontinuidade das atividades operacionais indispensáveis ao bom funcionamento da instituição.

O colaborador responsável pela coordenação das atividades e da comunicação em situações contingenciais é o responsável pelas atividades de Risco e *Compliance*, ou, na sua ausência, os gestores de cada área da organização. É de responsabilidade destes funcionários tomar as devidas decisões e informar todos os membros da equipe afetados pelo ocorrido das medidas a se adotar.

Em situações de impossibilidade de acesso às instalações físicas do Cerus Bank, todos os colaboradores deverão se dirigir aos gestores responsáveis pela continuidade operacional da instituição. Outros fatores que podem motivar o acionamento do plano de contingência da companhia são problemas de origem técnica (falhas de *hardware* e *software*), ausências de pessoas chaves, e crises de infraestrutura.

O responsável pelo setor de risco e *compliance*, deve, em situações de risco, adotar as seguintes medidas:

- Compreender a natureza do risco e avaliar as diferentes formas que este pode impactar negativamente as atividades da instituição, consultando outros membros da equipe para desempenhar esta função, caso necessário;
- Definir as medidas a serem tomadas de forma a mitigar os impactos do ocorrido, e garantir o bom funcionamento e atendimento a clientes durante a situação de crise;
- Contatar os funcionários do Cerus Bank de modo geral e de maneira individualizada, de acordo com as prioridades definidas na etapa anterior, de forma a colocar em funcionamento as atividades definidas na etapa 2;
- Acompanhar o decorrer das atividades de maneira a certificar a retomada operacional da Companhia, e adotar medidas corretivas, caso necessário, até a conclusão da calamidade;
- Analisar e avaliar o ocorrido após sua conclusão, em conjunto com a equipe Cerus Bank, de forma a debater propostas sobre como aumentar a robustez operacional da instituição em situações semelhantes que possam vir a ocorrer futuramente.

Em casos de impedimento de acesso às instalações físicas do Cerus Bank, os colaboradores deverão conduzir normalmente suas atividades de forma remota, enquanto não receberem instruções que digam o contrário. Concomitantemente, os funcionários capazes deverão realizar melhores esforços para entrar em contato com o responsável do setor Compliance para se informar da situação e de como devem agir.

Devido à natureza independente dos sistemas da instituição, localizados inteiramente na nuvem, a impossibilidade de acesso físico ao Cerus Bank não implica necessariamente em risco de continuidade de suas operações. Semestralmente, todos os funcionários devem realizar o teste de trabalho remoto de forma a garantir a eficácia de suas funções quando desempenhadas em local e em máquinas diferentes do habitual.

14. PROGRAMAS DE TREINAMENTOS

O Cerus Bank executa um processo de treinamento inicial para todos seus integrantes quando ingressam na organização, com maior foco àqueles em gestão de riscos e operações – em especial aos que tenham acesso a informações confidenciais.

Assim que cada integrante é contratado, ele deve passar por treinamento geral sobre as atividades do Cerus Bank e sobre a regulamentação e autorregulamentação aplicável. Atenção especial deve ser dada para o treinamento e instrução às regras relativas à atividade de gestão de recursos de terceiros, perfil dos nossos clientes, políticas em gerais, procedimentos e processos internos. Durante o treinamento, o novo integrante terá a oportunidade de esclarecer quaisquer dúvidas relacionadas.

Não obstante, o Cerus Bank entende que é fundamental que todos os integrantes, especialmente aqueles que tenham acesso a informações confidenciais, tenham sempre conhecimento atualizado dos princípios éticos do Cerus Bank e das leis, regulamentações, instruções e normas relevantes. Neste sentido, o Cerus Bank adota um programa de reciclagem dos seus integrantes, na medida em que as regras e conceitos de que tratam esta Política sejam atualizados. O objetivo desta reciclagem é fazer com que os membros da instituição estejam sempre atualizados.

15. PENALIDADE

Violações a esta Política devem resultar em advertência, revisão de responsabilidade, suspensão, ou dispensa, conforme o caso, do contrato de trabalho e/ou PJ, por recomendação do responsável por *Compliance* ou de qualquer dos diretores responsáveis, submetidas primeiramente ao Comitê de *Compliance* e para posterior decisão final do Comitê Executivo.

O Cerus Bank não assume a responsabilidade de integrantes que transgridam a lei ou cometam infrações no exercício de suas funções. Caso o Cerus Bank venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus integrantes, pode vir a exercer o direito de regresso em face dos responsáveis.

O integrante que tiver conhecimento ou suspeita de ato não compatível com os dispositivos desta Política, deve reportar, imediatamente, tal acontecimento ao responsável de *Compliance*. O integrante que se omitir de tal obrigação poderá sofrer além de ação disciplinar, rescisão de contrato ou mesmo demissão por justa causa. Adicionalmente, os integrantes que, de boa-fé, reportem uma possível violação devem ser protegidos e não sofrerão qualquer penalidade.

16. MONITORAMENTO E INFORMAÇÃO

Repetição periódica da avaliação e comunicação da informação gerada no processo de identificação, análise e tratamento de não conformidades às partes interessadas.

17. INFORMAÇÃO E COMUNICAÇÃO

Após serem identificadas, as não conformidades devem ser devidamente reportadas, cabendo ao Comitê de *Compliance* e Comitê Executivo, quando necessário, tomar as ações corretivas que julgar adequadas e de maneira tempestiva.

18. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

É dever de todos os integrantes do Cerus Bank, levar em consideração e respeitar as tratativas constantes na Lei em pauta.

19. REVISÃO

O Cerus Bank e o ambiente no qual atua são dinâmicos. Para assegurar que evoluções sejam incorporadas a esta Política continuamente, que deve refletir as melhores práticas de mercado e da companhia, revisões deverão ser efetuadas com uma periodicidade mínima anual.

A responsabilidade pela elaboração e atualização desta Política é da área de *Compliance* do Cerus Bank, que encaminhará proposta formal para avaliação e aprovação pelo Comitê de *Compliance* e posterior avaliação e aprovação do Comitê Executivo da instituição.

VICTOR VOLPATO

DIRETOR VICE-PRESIDENTE

Victor Volpato
CERUSBANK INSTITUICAO DE PAGAMENTO S.A

Data da última atualização: 18 de abril de 2022.

AGRADECEMOS POR VOCÊ TER LIDO NOSSA POLÍTICA DE CONTROLE INTERNO, RISCOS E COMPLIANCE DO CERUS BANK

BEM-VINDO(A) À FAMÍLIA CERUS!

CERUSBANK INSTITUIÇÃO DE PAGAMENTO S.A