ABRANGÊNCIA: UNICRED DTVM

DATA DE PUBLICAÇÃO: 17/10/2024 | VERSÃO: 01

POLÍTICA DE CONTROLES INTERNOS

UNICRED

Emissor: UNICRED DTVM | **Revisor:** Grupo de Trabalho Normativo | **Aprovador:** Política aprovada pelo DIREX da DTVM em 17/10/2024 pela ata nº09.

SUMÁRIO

1. OBJETIVO

Essa política tem como principal objetivo dispor sobre os procedimentos realizados pela UNICRED Distribuidora de Títulos e Valores Mobiliários Ltda. ("UNICRED DTVM") para um programa efetivo de governança corporativa e gerenciamento de riscos robustos, por meio de sua estrutura integrada e contínua de controles internos.

O documento dispõe sobre a implementação, manutenção e responsabilidades dentro do sistema de controles internos da UNICRED DTVM, bem como o acompanhamento da implementação e aplicação das regras, exigências e vedações previstas na regulamentação vigente. Destaca-se também as responsabilidades que envolvem os processos da Unicred DTVM, Participante de Negociação (PN) e o parceiro contratado na condição de Participante de Negociação Pleno (PNP), para prestação de serviços de back office, incluindo a disponibilização de infraestrutura de atendimento dos clientes da DTVM e serviços necessários para conexão e realização de negócios nos mercados administrados pela B3, devidamente cadastrado na B3 – Brasil, Bolsa, Balcão.

Conforme exigido pela Comissão de Valores Mobiliários ("CVM") na Resolução 35 de maio de 2021, os procedimentos de controles internos devem ser escritos, passíveis de verificação e estar disponível para consulta dos administradores, funcionários, prepostos e prestadores de serviços relevantes, da CVM, das entidades administradoras dos mercados organizados e da entidade autorreguladora.

2. REGULAMENTAÇÃO APLICÁVEL

- Resolução do Conselho Monetário Nacional (CMN) nº 4968/21 e suas alterações;
- Circular do Banco Central do Brasil (BCB) nº 3.467/09 e suas alterações;
- Resolução da Comissão de Valores Mobiliários (CVM) nº 35/21;
- Código de Distribuição – ANBIMA;
- Código ANBIMA de certificação;
- Roteiro PQO – Programa de Qualificação Operacional.

3. ESCOPO E ABRANGÊNCIA

A Política se aplica aos colaboradores da UNICRED DTVM, incluindo os prestadores de serviço e administradores.

Todas as modalidades de negócios e serviços estão suportadas por políticas e procedimentos internos, devidamente aprovados pela alta administração, que preveem as diretrizes a serem observadas em todas as operações e negócios conduzidas internamente, que visam manter elevada aderência regulatória e padrões de excelência em termos de conduta e ética nos negócios.

4. AMBIENTE DE CONTROLE

A UNICRED DTVM , instituição que faz parte do conglomerado da Unicred do Brasil, estabeleceu um ambiente de controle que visa assegurar a conformidade da instituição com leis e normas estabelecidas pelos órgãos reguladores e autorreguladores, tais como, Conselho Monetário Nacional (CMN), Banco Central do Brasil (BCB), Comissão de Valores Mobiliários (CVM), Brasil Bolsa, Balcão (B3), Bm&fBovespa Supervisão de Mercados (BSM) e da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA).

Ressalvamos que nos referimos ao ambiente de controle da UNICRED DTVM, e nesse caso aos controles aqui executados. Quanto ao ambiente de controle existente no prestador de serviço de PNP, para os processos operacionais contratados em SLA (*Service Level Agreement*), é de sua responsabilidade a adequação às normas regulamentares.

Em consonância com os mais elevados padrões de qualidade, o ambiente de controle da UNICRED DTVM deve:

- Garantir estrutura apropriada que permita a implementação e a adequada manutenção de controles que mitiguem os riscos identificados e os mantenham nos padrões definidos;
- Assegurar adequada atribuição de responsabilidades, preservando a independência entre as áreas de controle e as áreas de negócios, eliminando potenciais conflitos de interesses existentes;
- Garantir elevados padrões de integridade e valores éticos na instituição, disseminando uma cultura de controles internos de forma ampla e permanente entre os colaboradores e prestadores de serviços da UNICRED DTVM;
- Garantir a manutenção de canal permanente de comunicação entre os colaboradores das diversas áreas, gestores e Diretoria, assegurando o livre acesso da área de Compliance em situações de denúncias, alertas e comunicações de eventuais não conformidades observadas;
- Assegurar programas de treinamento regulares para todos os colaboradores da instituição, que possibilitem o perfeito entendimento das suas responsabilidades e deveres previstos na regulamentação vigente, com reciclagens e atualizações frequentes;

- Ser contínuo e efetivo, definindo as atividades de controle para todos os níveis de negócios e para todos os riscos aos quais a instituição está exposta;
- Integrar as atividades rotineiras das áreas relevantes da instituição; e garantir que sejam revisados e atualizados periodicamente;
- Divulgar o código de ética ou documento equivalente;
- Identificar e avaliar continuamente os fatores internos e externos que possam afetar adversamente a realização dos objetivos da instituição e, quando aplicável, do grupo econômico que esta integra.

5. CONTROLES INTERNOS

A UNICRED DTVM atua no âmbito da B3 como Participante de Negociação (PN), tendo como prestador de serviços de PNP (Participante de Negociação Pleno) o parceiro BTG Pactual, responsável pelos serviços de *back office*, incluindo a disponibilização de infraestrutura de atendimento dos clientes da DTVM e serviços necessários para conexão e realização de negócios nos mercados administrados pela B3, com o modelo de negócio PNP PN aberto.

Tanto a UNICRED DTVM (PN) quanto o BTG Pactual (PNP) possuem estruturas de controles internos individuais e deverão emitir relatórios de controles internos próprios anualmente, conforme estabelecidos na Resolução CVM nº 35. As duas instituições designam individualmente diretores responsáveis por controles internos e pela Resolução CVM nº35, bem como possuem Diretor de Relações com o Mercado na B3 para cumprimento das regras de permanência no mercado da B3.

Na Governança de Gestão de Riscos, a UNICRED DTVM pratica o conceito de "linhas de defesa", que proporciona o ambiente de controle necessário para prevenir e combater ações de natureza ilícita, bem como assegurar que os principais riscos envolvidos nas operações sejam conhecidos, monitorados e tratados adequadamente. Consideramos assim essas linhas de defesa:

i. Primeira linha: Áreas de Negócio - Detêm e administra os seus riscos;

ii. Segunda linha: Controles internos, Gerenciamentos de riscos e Compliance - Definem a estratégia e estrutura de gerenciamento de risco, coordenam os limites operacionais desafiando e monitorando as funções da primeira linha;

iii. Terceira linha: Auditoria Interna - Provém garantias independentes da estrutura de gerenciamento de riscos.

Vale lembrar que o modelo de negócios da UNICRED DTVM prevê o atendimento aos seus clientes, que na sua totalidade são cooperados associados às cooperativas ligadas ao sistema da Unicred Brasil.

5.1. ATIVIDADES DE CONTROLE

A equipe de Controles Internos e Compliance da UNICRED DTVM é responsável por:

- Garantir a efetividade dos controles internos que estão sob responsabilidade do PN;
- Acompanhar os controles que estão sob a responsabilidade do PNP;

- Formalizar suas atividades por meio de políticas e manuais contendo normas e procedimentos definidos e atualizados;
- A capacitação técnica, certificação e treinamento dos funcionários responsáveis pelo processamento das operações nos segmentos de atuação, conforme requisitos do Banco Central do Brasil, CVM, B3 e ANBIMA;
- No ambiente de controles do PN, realizar manutenção dos planos de contingência com acompanhamento e avaliação das atualizações e dos resultados dos testes em relação aos objetivos estabelecidos;
- Com relação a Governança de TI (Tecnologia da Informação), o PN é responsável pela segurança do seu ambiente tecnológico, contemplando a elaboração da sua própria política de segurança da informação, política de segurança cibernética, controle de acessos e continuidade dos negócios;
- Com relação a questões comportamentais e situações previstas no Código de Ética e Conduta, acompanhar:
    - A obrigatoriedade de comunicação tempestiva ao adequado nível gerencial, por parte dos funcionários, quanto a problemas nas operações, situações de não conformidade com os padrões de conduta definidos pela instituição e violações das políticas da instituição ou de disposições legais e regulamentares;
    - Proibição de estabelecimento de metas de desempenho que incentivem a tomada de riscos em desacordo com os níveis determinados pela alta administração;
- Revisar e atualizar periodicamente os sistemas de controles internos, com a inclusão de medidas relacionadas a riscos novos ou não abordados anteriormente, bem como mitigar os riscos não tolerados e não controlados;
- Acompanhar ações que desestimule o envolvimento da instituição em atividades indevidas ou ilícitas, em especial as relacionadas aos riscos sociais, ambientais e climáticos;
- Manter fluxos de informações adequados para que os objetivos, estratégias, expectativas, políticas e procedimentos estabelecidos pelos superiores cheguem aos funcionários e as informações relevantes sejam compartilhadas entre os componentes organizacionais;
- Prover sistemas de informação confiáveis e as respectivas medidas de segurança e monitoramento independente para sua manutenção, para aqueles contratados pelo PN;
- Aplicar testes periódicos de segurança para os sistemas de informações e de tecnologia;
- Realizar avaliações periódicas, acerca da eficácia dos sistemas de controles internos e dos principais riscos associados às atividades da instituição.
-

5.2. PROTEÇÃO DA INFORMAÇÃO

A UNICRED DTVM adota medidas para garantir que a Política de Segurança da Informação esteja adequada a melhores prática de mercado, sendo assim:

- Toda aquisição ou locação de recursos de informática (equipamentos, softwares, sistemas, nuvens de serviços) é previamente consentida pela área de Tecnologia da Informação, mediante aprovação prévia da Diretoria;
- Todo recurso de informática é inventariado e qualquer alteração em sua configuração original só pode ser realizada pela área da Tecnologia da Informação;
- Todos os programas de computador desenvolvidos para a UNICRED DTVM são de propriedade da mesma e obedecem aos critérios legais e melhores práticas com modelos de desenvolvimento seguro;
- É responsabilidade do usuário não instalar programas em condição ilegal de uso ou não autorizados pela área de Tecnologia da Informação;
- A área de Tecnologia da Informação realiza o monitoramento da instalação de programas ilegais ou não autorizados;
- A aquisição, homologação e instalação de licenças de programas segue normas e procedimentos definidos pela área de Tecnologia da Informação da UNICRED DTVM;
- As licenças de programas de computador usados por terceiros são de inteira responsabilidade deles, mas devem obedecer a critérios mínimos de Segurança da Informação;
- Os usuários são responsáveis pelas informações armazenadas nos equipamentos que utilizam, bem como a manutenção dos arquivos armazenados em pastas. O modo mais seguro de armazenar documentos e informações é utilizando pastas e diretórios disponíveis em rede.

A UNICRED DTVM compromete-se a manter a integridade das informações, para isso adota critérios, utiliza-se de ferramentas que tem por objetivo garantir a segurança das informações em posse da instituição.

5.3. SIGILO DAS INFORMAÇÕES DECORRENTE DA PRESTAÇÃO DE SERVIÇOS

No mercado no qual a UNICRED DTVM está inserido, o sigilo proteção das informações é imprescindível, por isso, todas as informações classificadas nas disposições gerais deste documento recebem atenção em relação ao seu uso e divulgação.

Além disso, na UNICRED DTVM são tratadas também como informações confidenciais e restritas as seguintes, sem prejuízo de outras em ocorrências de novos negócios:

- Registros de ocorrências;
- Estudos internos usados para tomadas de decisão;
- Acordos financeiros em geral;
- Documentos de terceiros e clientes;
- Workflows internos;
- Dados estatísticos gerenciais diversos;
- Toda informação cadastral de clientes;
- Base de cadastro, financeira, controladoria e contábil;

- Inteligência de Negócio;
- Contas a pagar e folha de pagamento, serão divulgadas apenas com partes autorizadas. Dados de operações de clientes e posições de custódia.

5.4. MONITORAMENTO DE MENSAGENS ELETRÔNICAS

- Os sistemas de mensageria e outros são gravados e disponibilizados sempre que solicitado;
- As mensagens são mantidas armazenadas durante 5 anos.

5.5. INVENTÁRIO DE ATIVOS

A UNICRED DTVM mantém inventário atualizado dos ativos de informação contendo recursos de hardware, software, aplicações de negócio, equipamentos de rede, recursos humanos, instâncias virtuais em nuvem, instalações físicas e itens de configuração relevantes para a empresa como terceiros e fornecedores.

5.6. SENHAS

- As senhas são pessoais e intransferíveis, é expressamente proibido o compartilhamento de senha pessoal. Todos os colaboradores que têm acesso a contas de sistemas deverão ser claramente identificados;
- Todas as senhas em nível de usuário, por exemplo, senha de rede deve ser alteradas, no máximo, a cada noventa dias, exceto nos casos de senhas para plataformas eletrônicas;
- As senhas não devem ser anotadas ou inseridas em mensagens de e-mail ou outras formas de comunicação eletrônica;
- As senhas devem possuir no mínimo seis caracteres contendo letras maiúsculas, números e caracteres especiais;
- As senhas devem possuir histórico mínimo de seis senhas utilizadas, exceto nos casos de senhas para plataformas eletrônicas;
- As senhas nunca devem ser escritas ou armazenadas em sistemas sem criptografia;
- As senhas serão bloqueadas após cinco tentativas incorretas;
- O desbloqueio do usuário será efetuado pelo administrador da rede. Em plataformas eletrônicas o desbloqueio deverá ser mediante a confirmação de dados do usuário, tais como, dados pessoais e cadastrais;
- Constitui obrigação exclusiva do usuário, zelar pela guarda e conservação de sua senha, cabendo ao usuário informar ao departamento de Tecnologia sobre suspeitas e

uso, ou efetivo ou indevido. O uso indevido da senha ou credencial de acesso por terceiros não exime a responsabilidade do usuário;
- Todas as senhas devem ser tratadas como informações confidenciais da UNICRED DTVM;
- Exceções a esta norma podem ser concedidas de acordo com cada cenário, havendo a necessidade de tratamento registrado de exceções.

5.7. ACESSO E RESTRIÇÃO DE ACESSO

A UNICRED DTVM restringe o acesso as informações e áreas físicas e eletrônicas apenas para colaboradores autorizados, fazendo o uso do princípio do menor privilégio. Por isso:

- Os crachás são pessoais e intransferíveis, sendo vedado o empréstimo;
- Os acessos são liberados e autorizados pela área administrativa e Controladoria, responsável pelo cadastro e liberação, conforme Norma Acesso Seguro aos Ambientes Internos.
- Não é permitido dar carona ou a entrada de pessoas não autorizadas nos ambientes controlados por dispositivos de controle de acesso (salvo exceções autorizadas quanto a visitas de fornecedores e clientes);
- Não é permitida a violação dos dispositivos de controle de acesso por qualquer motivo, exceto por manutenção;
- A concessão de acesso à rede, programas, cadastros sistemas são feitas por meio de análise da Matriz de Segregação de Função de modo a identificar a legitimidade do acesso em questão;
- Todo acesso a informações da UNICRED DTVM, feitos fora da matriz, devem ser autorizados pelo Compliance e Gestor da Informação;
- Todos os acessos são passiveis de auditoria, seja navegação, acesso físico e acesso lógico, devendo ser disponibilizado ao Compliance a "trilha de auditoria e/ou log", caso seja solicitado;
- Todos os acessos a sistemas estão sujeitos à revisão minimamente anual para verificação do perfil do usuário que devem ser validadas pelos respectivos gestores;
- Todos os casos de desligamentos e/ou transferência de colaboradores devem ser imediatamente comunicados por Recursos Humanos para que seus acessos sejam bloqueados e/ou reformulados;
- Não é permitido o desbloqueio de portas (salvo exceção quando acompanhado por responsável por motivos previamente avisados como manutenções);
- Não é permitida a permanência de portas abertas nos ambientes operacionais, administração de fundos e ambiente computacional da UNICRED DTVM.

Todos os acessos físicos e lógicos devem ser solicitados para a área de Suporte. Para conceder o acesso, a área de Suporte verifica as permissões constantes na Matriz de Segregação de Funções e Acessos. Caso a solicitação não esteja prevista na Matriz, a área de Suporte solicita autorização para a área de Compliance, que analisará, caso a caso, em

conjunto com o gestor do solicitante. Caso a solicitação seja para acesso a informações confidenciais, reservadas ou privilegiadas que sejam essenciais para o desempenho das atividades, o usuário deverá assinar novo termo de confidencialidade sobre as informações a que terá acesso. Caso seja para uso temporário, os acessos devem ser retirados assim que as atividades tenham sido encerradas.

5.8. USO DE E–MAIL E INTERNET

A comunicação indevida por e-mail, sistema de mensagens ou acesso a sites não autorizados pode comprometer a Segurança da Informação da UNICRED DTVM, sendo assim são adotadas algumas premissas como:

- O acesso à internet dentro das dependências da UNICRED DTVM é classificado e bloqueado/permitido com base em categorias de Website com bloqueios em especial a (chats, redes sociais de entretenimento, webmails, etc.);
- Apenas o e-mail corporativo pode ser utilizado para troca de mensagens referentes a assuntos da UNICRED DTVM;
- Todos os colaboradores devem utilizar o e-mail disponibilizado pela UNICRED DTVM para fins profissionais, sendo proibido o uso para fins particulares;
- O acesso a sites disponíveis na rede mundial de computadores é restrito, visando a vulnerabilidade de alguns sites como rede sociais, sites de compra, entre outros;
- A UNICRED DTVM reserva-se o direito de monitorar o acesso à Internet e envio de mensagens eletrônicas, com o objetivo de proteger os dados da instituição;
- As caixas de e-mail utilizadas para recebimento e transmissão de ordens, instruções e confirmações são armazenadas pelo período de 5 anos.

5.9. FERRAMENTAS DE SEGURANÇA

A fim de evitar o vazamento de informações, fuga de dados, a integridade e guardas destas, é essencial a utilização de ferramentas tecnológicas destinadas a proteção dos sistemas informatizados, da UNICRED DTVM:

- Backups regulares;
- Segurança de antivírus;
- Gerenciamento de Patch – proteção contra ameaças;
- Gestão de vulnerabilidade varredura do ambiente;
- Monitoramento de comportamento suspeito (Internet, E-mail, Mensagens, Redes Sociais etc.);
- Criptografia;
- Bloqueio de gravações (saídas USB, pen drives, HD etc.).

O tráfego de dados, preservação de documentos e rastreabilidade das informações são garantidas com a utilização do Sistema especializado que:

- Rastreia o ciclo de vida de um documento (qualquer alteração realizada por funcionários e clientes pode ser verificada);
- Rastreio de envio do documento para e-mails particulares, túneis, etc.;
- Mantém arquivos, documentos e dados armazenados criptografados.

5.9. DESCARTE DE EQUIPAMENTOS E DESTRUIÇÃO DE INFORMAÇÕES

Toda mídia e papel deverá ser descartada quando se tornar desnecessária. A mídia não deverá ser reutilizada, doada para caridade ou descartada sem a devida autorização da área Tecnologia da Informação. Para minimizar o risco de divulgação acidental de informação sigilosa, a área Tecnologia da Informação deverá garantir a execução de uma forma segura de descarte (ou seja, incineração, fragmentação ou limpeza completa), destruindo completamente e de maneira irreversível toda e qualquer informação da UNICRED DTVM. O descarte de papel deverá ser feito após a trituração de seus conteúdos de modo que se tornar ilegível e/ou irrecuperável.

A reutilização, venda ou doação assistencial de computador fora de uso, poderá ocorrer, se não houver qualquer risco de exposição de dados sigilosos, ou danos organizacionais potenciais à informação previamente abrigada nesses sistemas.

5.10. SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

A empresa se compromete a aplicar as medidas técnicas e organizacionais aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão de tais dados.

A UNICRED DTVM tem a responsabilidade de cuidar dos dados pessoais e utilizá-los para finalidades lícitas, conforme descrito nesta Política. Para garantir a sua privacidade e a proteção dos seus dados pessoais, adotamos práticas de segurança adequadas para o nosso mercado, dentre as quais:

- Criptografia e sistemas de dupla autenticação nos ambientes das nossas Plataformas;
- Treinamentos e políticas de conscientização, para mantermos nossos colaboradores atualizados sobre como evitar riscos ao Titular dos Dados e identificar ameaças e atividades maliciosas;
- Controles e privilégios de acesso a Dados Pessoais, de modo que cada colaborador somente pode acessar os dados estritamente necessários para o desempenho de suas funções;
- Controle e monitoramento preventivo de incidentes de segurança, incluindo vazamento de dados, realizado pelo nosso time de Segurança da Informação e por ferramentas automatizadas de segurança reconhecidas pelo mercado.

5.11. SEGURANÇA DA INFORMAÇÃO

As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação da UNICRED DTVM deverão considerar, prioritariamente, os objetivos estratégicos, os processos críticos, os requisitos legais e a estrutura da empresa, além de estarem alinhadas a esta Política. Esse processo deverá ser contínuo e aplicado na implementação, operação, manutenção, controle e melhoria contínua do Sistema de Gestão de Segurança da Informação e do Sistema de Gestão de Continuidade de Negócio.

A UNICRED DTVM adota as melhores práticas de mercado, por isso promove a divulgação interna de sua Política de Segurança da Informação e oferece treinamento sobre o tema para todos os colaboradores e para garantir o sigilo das informações os colaboradores são orientados a:

- Não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;
- Não se apropriar para si ou para outro de material confidencial e/ou sigiloso da tecnologia que venha a ser disponível;
- Guardar os documentos relativos à sua atividade em local seguro e de acesso restrito apenas as pessoas previamente autorizadas;
- Assegurar que informações confidenciais não estejam expostas, a outros profissionais ou a terceiros em trânsito na UNICRED DTVM nas dependências da empresa, em períodos de ausência de seu local físico de trabalho;
- Não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas;
- Bloquear o computador quando se ausentam de sua mesa.

5.12. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A UNICRED DTVM deverá definir e elaborar os documentos, análises e planos necessários para composição do seu Plano de Continuidade de Negócios, que deverá ser composto, pela Business Impact Analysis – BIA e pelos Planos de Continuidade de Negócios necessários, de acordo com as avaliações realizadas, de forma a assegurar o planejamento, preparação, resposta e recuperação diante de indisponibilidades:

- Identificação, classificação e documentação dos processos considerados críticos e vitais para continuidade do negócio;
- Definição e formalização das estratégias a serem adotadas num nível previamente definido, em casos de incidentes e crises, relacionadas aos processos críticos e a continuidade de suas atividades;

- Os planos definidos deverão ser testados e revisados periodicamente, visando a efetividade das estratégias definidas, a adequada participação e comunicação dos envolvidos e o aumento da resiliência organizacional;
- A Unicred DTVM deverá fomentar no âmbito da sua instituição, a importância sobre o aculturamento quanto ao tema GCN, a elaboração e atualização dos planos necessários e aumento da resiliência organizacional.

5.13. RELATÓRIO DE CONTROLES INTERNOS

A Área de Controles Internos deve realizar procedimentos de monitoramento dos processos operacionais e de suporte executados no ambiente de controles da UNICRED DTVM, mediante atividades contínuas, avaliações independentes ou a combinação de ambas, que podem incluir análises de variância, comparações das informações oriundas de fontes diferentes e registro de ocorrências.

No caso de controles executados no BTG Pactual (PNP), a UNICRED DTVM acompanha casos de exceções envolvendo os processos operacionais contratados no SLA, por meio documentos / relatórios ou por meio de agenda de reuniões para reporte, entre as equipes de Compliance das instituições.

Os resultados, com ressalvas sobre o ambiente de controle, se PN ou PNP, devem ser registrados em relatório específico de revisão dos controles internos, emitido anualmente, que permita a identificação e a correção tempestiva de eventuais deficiências de controle e o gerenciamento do risco operacional. O Relatório Anual de Controles Internos deve ser emitido pelo Diretor de Compliance, Riscos e PLD e ser encaminhado ao Comitê de Compliance e Controles Internos, contendo pelo menos:

- Descrição detalhada e atualizada dos controles internos implantados, metodologia aplicada para realização dos exames realizados, procedimentos realizados para análise das deficiências encontradas;
- Detalhamento dos testes realizados e das conclusões obtidas quanto à eficiência e eficácia dos controles internos envolvendo: as atividades de cadastro de clientes; conheça seu cliente (KYC); a transmissão e execução de ordens; especificação de comitentes; *suitability;* PLD/CFT; certificação de profissionais; contratação de prestadores de serviços; operações com pessoas vinculadas; o repasse de operações; o pagamento e recebimento de valores; normas de conduta e manutenção de arquivos; o monitoramento da infraestrutura de tecnologia da informação; segurança da informação;
- A avaliação sobre a adequação e a efetividade dos sistemas de controles internos;
- Avaliação de riscos para UNICRED DTVM em relação aos seus controles internos e quanto à sua vulnerabilidade a ataques cibernéticos;
- As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronograma de saneamento, quando for o caso;

- A manifestação dos responsáveis pelas correspondentes áreas a respeito das deficiências encontradas em verificações anteriores e das medidas efetivamente adotadas para saná-las;
- Manifestação do Diretor responsável pela Resolução 35/21 da CVM a respeito das deficiências encontradas, contendo no mínimo: informação sobre o andamento ou sobre a eventual conclusão das ações planejadas para saneamento das deficiências identificadas no exercício anterior; relação às deficiências apontadas nos relatórios anteriores, informar se os cronogramas de saneamento foram implementados e o resultado das ações adotadas para sanar as deficiências; avaliação sobre a evolução da UNICRED DTVM no cumprimento das exigências regulatórias; avaliação sobre a adequação do plano de continuidade de negócios, indicando as necessidades de aperfeiçoamento, quando necessário.

O documento deve ser submetido à Diretoria e permanecer à disposição do Banco Central do Brasil, CVM, B3, BSM, ANBIMA, por, pelo menos, o prazo de cinco anos.

5.14. COMITÊ DE CONTROLES INTERNOS, COMPLIANCE E RISCOS

A UNICRED DTVM possui Comitê de Controles Internos, Compliance e Riscos, que será composto pela Diretoria, conforme indicada em seu Contrato Social, pelo Diretor de Compliance, Risco e PLD e por membros seniores da Equipe de Compliance e Risco, escolhidos pelo Diretor de Compliance, Risco e PLD e deverá analisar e debater possíveis falhas e oportunidades de aprimoramento nos controles internos da UNICRED DTVM., entre outros assuntos relacionados à estrutura de controles, conforme descrito abaixo, além dos demais assuntos pertinentes à gestão de riscos, conforme Política de Gestão de Risco da UNICRED DTVM.

São atribuições do Comitê de Controles Internos e Compliance da UNICRED DTVM relacionadas a esta Política:

- Zelar, por meio de supervisão, pelo cumprimento e efetividade dos procedimentos previstos nas políticas, manuais e demais documentos corporativos referentes ao ambiente de controles da UNICRED DTVM;
- Aprovar regras e procedimentos referentes ao ambiente de controles internos;
- Analisar eventuais situações indicadas pelo Diretor de Compliance, Risco e PLD sobre as atividades e rotinas de Compliance;
- Revisar as metodologias e parâmetros de controle existentes;
- Analisar eventuais casos de infringência das regras descritas nesta política, e manuais internos da UNICRED DTVM, das regras contidas na regulamentação em vigor, ou de outros eventos relevantes e definir sobre as ações e sanções a serem aplicadas.

A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos nesta política é de responsabilidade Diretor de Compliance, Riscos e PLD,

conforme definido pelo Comitê., garantido aos envolvidos, contudo, amplo direito de defesa.

Podem ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou exclusão por justa causa, sem prejuízos do direito da UNICRED DTVM de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

As reuniões do Comitê de Controles Internos, Compliance e Riscos serão realizadas trimestralmente, ou sob demanda, e suas deliberações serão consignadas em atas e/ou registradas por e-mail e arquivadas na sede da UNICRED DTVM.

5.15. COMITÊ DE PLD

A UNICRED DTVM possui Comitê de PLD, que será composto pela Diretoria, conforme indicada em seu Contrato Social, pelo Diretor de Compliance, Risco e PLD.

As reuniões do Comitê de PLD serão realizadas mensalmente, ou sob demanda, e suas deliberações serão consignadas em atas e/ou registradas por e-mail e arquivadas na sede da UNICRED DTVM.

A pauta do comitê deve contemplar, entre outras informações internas, os relatórios emitidos pelo BTG Pactual informando a situação do processo de monitoramento de operações atípicas e eventuais casos passíveis de comunicação ao COAF ou, se for o caso, informação da não ocorrência de suspeitas de situações caracterizadas como Lavagem de Dinheiro ou Financiamento ao Terrorismo.

5.16. ESTRUTURA DE GOVERNANÇA

A Diretoria da Instituição é responsável por garantir a existência de estrutura apropriada para o bom desempenho do Sistema de Controles Internos, assegurar a disseminação da cultura de controles por meio da capacitação dos profissionais encarregados pelos controles internos e garantir a atuação efetiva e independente da auditoria interna sobre o ambiente de controle e do gerenciamento de riscos, além de se envolver ativamente na definição dos sistemas de controles internos promovendo:

- Elevados padrões éticos e de integridade;
- A disseminação da cultura organizacional com ênfase na relevância dos sistemas de controles internos e respectivo engajamento dos envolvidos;
- A manutenção de estrutura organizacional adequada para garantir a qualidade e a efetividade dos sistemas e processos de controles internos;
- A garantia de recursos adequados e suficientes para o exercício das atividades relacionadas aos sistemas de controles internos, de forma que ocorram de maneira independente, objetiva e efetiva;

- Tomar as medidas necessárias para identificar, medir, monitorar e controlar os riscos de acordo com os níveis de riscos definidos;
- Providenciar que as falhas identificadas sejam tempestivamente corrigidas;
- Deliberar o monitoramento, adequação e a eficácia dos sistemas de controles internos;
- Promover que os sistemas de controles internos sejam implementados e mantidos de acordo com o disposto neste documento.

6. INFORMAÇÃO E COMUNICAÇÃO

As informações pertinentes a controles internos devem ser identificadas, coletadas e comunicadas de forma coerente e tempestiva, a fim de permitir que colaboradores e prestadores de serviços cumpram suas responsabilidades.

A comunicação deve fluir em todos os níveis organizacionais, promovendo a consistência e tempestividade das informações para a tomada de decisões da Diretoria, por meio de processo de comunicação confiável, oportuno, compreensível e acessível a todos envolvidos e ao público externo quando aplicável.

7. CONTROLE DA POLÍTICA

Esta Política está aprovada pela Diretoria de Controles Internos e será publicada e comunicada para todos os colaboradores e partes externas relevantes para o necessário cumprimento.

A Política entra em vigor a partir da data de sua publicação e será revisada e aprovada pela Diretoria anualmente. Caso mudanças regulatórias ocorrerem em período inferior o documento deverá contemplar tais alterações para assegurar a sua contínua pertinência, adequação e eficácia.

DATA	DESCRIÇÃO	APROVADOR
17/10/2024	Política de Controles Internos	DIREX da DTVM em 17/10/2024 na Ata nº 09/2024.


UNICRED