



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA



Diretoria: 04 Compliance e Riscos
Área: 01 Compliance
Título: 01 CODIGO PSIC

Publicação: 05/2024
Atualização: 05/11/2025
Versão: 004

INDICE

1. OBJETIVO
2. ABRANGÊNCIA
3. MISSÃO
4. BASE LEGAL
5. TERMOS E DEFINIÇÕES
6. PRINCÍPIOS
7. DIRETRIZES
8. PAPÉIS E RESPONSABILIDADES DAS ÁREAS ENVOLVIDAS
9. GERENCIAMENTO DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA
10. GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO
11. GERENCIAMENTO DA SEGURANÇA CIBERNÉTICA
12. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E COMPUTAÇÃO NA NUVEM
13. CONTRATAÇÃO DE SERVIÇOS RELEVANTES PRESTADOS POR TERCEIROS
14. SANÇÕES ADMINISTRATIVAS
15. DECLARAÇÃO DE RESPONSABILIDADE
16. DIVULGAÇÃO DESTA POLÍTICA
17. VIGÊNCIA E APROVAÇÃO DESTA POLÍTICA
18. ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA
19. ANEXO II – DIVULGAÇÃO DAS LINHAS GERAIS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA



Diretoria: 04 Compliance e Riscos
Área: 01 Compliance
Título: 01 CODIGO PSIC

Publicação: 05/2024
Atualização: 05/11/2025
Versão: 004

1. OBJETIVO

A presente Política visa estabelecer princípios e diretrizes para a preservação e proteção das informações de Clientes, Colaboradores, Fornecedores, Parceiros, Partes Interessadas e da própria instituição Dillon DTVM, contra ameaças e riscos relacionados à segurança da informação e cibernética. Além de assegurar a confidencialidade, integridade e a disponibilidade da informação, a continuidade do negócio, e o conformidade à legislação vigente, normas e boas práticas de mercado.

Esta Política visa implementar controles e procedimentos que reduzam a vulnerabilidade da Dillon DTVM a incidentes, e regulamenta os requisitos para a contratação de serviços de processamento e armazenamento de dados, bem como de computação em nuvem, considerando a complexidade do modelo de negócios, das atividades e dos processos da instituição.

2. ABRANGÊNCIA

Esta Política é aplicável a todos os Colaboradores, Clientes, Prestadores de Serviços e Parceiros, sócios da Dillon DTVM, independentemente da estruturação em unidades físicas, virtuais de forma de acesso, local ou remoto ao ambiente da Dillon DTVM.

É de responsabilidade de todos os Colaboradores o conhecimento, a compreensão e a busca de meios para proteger a Dillon DTVM contra práticas que possam infringir os riscos de Responsabilidade Social, Ambiental e Climática. As leis e regulamentos atrelados a estas áreas, bem como as regras desta Política, devem ser obrigatoriamente cumpridos por todos os Colaboradores.

Todos os Colaboradores devem aderir expressamente à esta Política por intermédio da assinatura – física ou eletrônica – do termo cujo modelo segue ao final deste documento.

3. MISSÃO

Todos os envolvidos, direta ou indiretamente, na utilização ou suporte aos sistemas, à infraestrutura ou às informações da Dillon DTVM devem:

- (i) cumprir rigorosamente as normas e procedimentos estabelecidos nesta Política, assegurando o uso adequado das informações e dos sistemas associados;
- (ii) comunicar imediatamente às áreas responsáveis qualquer falha em dispositivos, serviços ou processos relacionados à Segurança da Informação e Segurança Cibernética, para que ações corretivas sejam tomadas com agilidade;
- (iii) tratar as informações protegidas por esta Política como patrimônio estratégico da Dillon DTVM, garantindo sua segurança, integridade e disponibilidade, conforme sua classificação e importância.

4. BASE LEGAL

Dentre as principais normas disciplinadoras do mercado financeiro no que tange à Segurança da Informação e Segurança Cibernética, vale destacar:

- (i) **Resolução CVM nº 35/2021:** estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários.
- (ii) **Resolução CMN nº 4.557/2017:** dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.
- (iii) **Resolução CMN nº 4.893/2021:** dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

5. TERMOS E DEFINIÇÕES

5.1. Para fins dessa Política, são considerados:

5.1.1. **Administradores:** Diretores da Dillon DTVM.

5.1.2. **Ativos:** qualquer forma de dados que geram informações, incluindo documentos impressos, sistemas, *softwares*, bancos de dados, arquivos digitais, dispositivos móveis, entre outros.

5.1.3. **BCB:** Banco Central do Brasil.

5.1.4. **Clientes ou Usuários:** pessoas físicas ou jurídicas que contratam e utilizam os produtos e/ou serviços da Dillon DTVM.

5.1.5. **Colaboradores:** empregados, prestadores de serviços sem vínculo empregatício, trainees e estagiários que atuam na Dillon DTVM.

5.1.6. **Comitê de Segurança da Informação e Segurança Cibernética:** comitê formado por Colaboradores indicados pelos Administradores e aprovado pela Reunião de Diretoria de 05 de novembro de 2025, responsável por deliberar sobre temas relacionados à Segurança da Informação e Segurança Cibernética.

5.1.7. **Conta de Custódia:** guarda e administração de ativos financeiros registrados em nome de seus Clientes.

5.1.8. **Conta de Depósito:** registro de valores a favor dos seus Clientes, permitindo operações como depósitos, saques, transferências e pagamentos.

5.1.9. **CVM:** Comissão de Valores Mobiliários.

5.1.10. **Diretor responsável pela Segurança da Informação e Segurança Cibernética:** diretor designado para implementar, executar e manter esta Política, além de gerenciar o Plano de Ação e Resposta a Incidentes e convocar reuniões periódicas do Comitê de Segurança da Informação e Segurança Cibernética, quando implementado.

5.1.11. **Fornecedores:** pessoas físicas ou jurídicas, públicas ou privadas, nacionais ou estrangeiras, que fornecem produtos ou prestam serviços à Dillon DTVM.

5.1.12. **Distribuidora de Títulos e Valores Mobiliários:** para fins desta Política, a Dillon DTVM, atua com a intermediação de operações de compra e venda de títulos e valores mobiliários, gerenciando carteiras de ativos, oferecendo a custódia de títulos, exercendo o papel de agente fiduciário e administrando fundos de investimento, para facilitar o acesso dos seus Clientes aos diversos ativos financeiros.

5.1.13. **Gerenciamento de Ativos:** práticas adotadas pela Dillon DTVM para controlar ativos tangíveis e intangíveis (equipamentos, contratos, marcas, ferramentas, materiais e know-how), visando resultados sustentáveis para a operação.

5.1.14. **Informações Sensíveis:** informações estratégicas para os negócios e operações da Dillon DTVM, tangíveis por meio de transações, processamentos, bancos de dados e outros meios.

5.1.15. **Parceiros:** pessoas físicas ou jurídicas, públicas ou privadas, nacionais ou estrangeiras, que firmam contratos com a Dillon DTVM para colaborar com seus negócios mediante retribuição.

5.1.16. **Partes Interessada:** Colaboradores, sócios, Clientes, Fornecedores, Parceiros e a comunidade na qual a Dillon DTVM está inserida, e a sociedade em geral.

5.1.17. **Política:** esta Política de Segurança da Informação e Segurança Cibernética.

5.1.18. **Segurança Cibernética:** conjunto de tecnologias e processos destinados a proteger sistemas internos, computadores, redes e dados da Dillon DTVM contra ataques, danos, ameaças ou acessos não autorizados.

5.1.19. **Segurança da Informação:** conceitos, mecanismos e estratégias para proteger os Ativos da Dillon DTVM.

5.1.20. **Sistema do Mercado Financeiro e de Capitais:** serviços oferecidos pela Dillon DTVM relacionados à administração de carteiras de ativos, custódia de títulos, intermediação de operações financeiras e execução de transações de compra e venda de valores mobiliários.

5.1.21. **SMI:** Superintendência de Relações com o Mercado e Intermediários, essa área é responsável por supervisionar as atividades das instituições intermediárias no mercado de capitais, como corretoras, distribuidoras e outras entidades que atuam na intermediação de valores mobiliários.

5.1.22. **Tipo de métodos para ataques cibernéticos:** São formas que criminosos se utilizam para buscar acesso ao ambiente tecnológico das instituições, buscando, assim, os dados delas e de seus clientes, de modo a obter vantagem sobre eles (como, por exemplo, mas não se limitando a, cobrança de resgata, uso em operações fraudulentas etc.):

- (i) **Malware:** *softwares* desenvolvidos para corromper computadores e redes:
 - i. vírus: software que causa danos a máquina, rede, *softwares* e banco de dados;
 - ii. cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
 - iii. *spyware*: software malicioso para coletar e monitorar o uso de informações; e
 - iv. *ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- (ii) Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
 - i. *pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
 - ii. *phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
 - iii. *vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
 - iv. *smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
- (iii) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- (iv) Ataques de DDoS (Distributed Denial of Services) e *botnets* – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- (v) Invasões (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Transação: operação financeira ou negociação realizada no mercado financeiro ou de capitais que envolva a intermediação, administração ou execução de ativos financeiros.

6. PRINCÍPIOS

6.1. A Dillon DTVM está comprometida em garantir a segurança e o tratamento adequado das informações. Para isso, adota práticas fundamentadas nos seguintes princípios:

- (i) Autenticidade: garantia de identificar e autenticar usuários, entidades, sistemas ou processos que tenham acesso às informações;
- (ii) Confidencialidade: garantia de que apenas pessoas autorizadas terão acesso às informações, e somente quando houver necessidade;
- (iii) Disponibilidade: garantia de que as informações estarão acessíveis às pessoas autorizadas sempre que necessário; e
- (iv) Integridade: garantia de que as informações permanecerão exatas, completas e protegidas contra modificações indevidas.

7. DIRETRIZES

7.1. Esta Política, atende às Resoluções CMN nº 4.893/2021 e CVM nº 35/2021, que dispõem sobre as seguintes diretrizes:

7.2. A Cultura de Segurança da Informação e Segurança Cibernética desenvolve e implementa iniciativas para promover a conscientização e boas práticas relacionadas à Segurança da Informação e Segurança Cibernética, incluindo:

- (i) programas de capacitação, treinamentos e avaliações periódicas de pessoal; e
- (ii) informações e orientações aos usuários finais sobre precauções no uso de produtos e serviços oferecidos pela Dillon DTVM.

7.3. Controles de Acesso e Confidencialidade:

- (i) garantir tratamento ético e sigiloso das informações, evitando acessos indevidos, modificações, destruições ou divulgações não autorizadas;
- (ii) assegurar que o acesso dos Colaboradores seja pessoal, intransferível e limitado aos recursos necessários; e
- (iii) implementar mecanismos de gerenciamento de senhas e uso seguro de credenciais.

7.4. Classificação de Dados: classificar os dados e informações de acordo com sua relevância e sensibilidade.

7.5. Compatibilidade de Controles: desenvolver o controle de dados de clientes, assegurando confidencialidade, integridade e disponibilidade das informações. Garantir que os procedimentos e controles estejam alinhados ao nível de complexidade e à estratégia de negócios exigidos pela Dillon DTVM.

7.6. Finalidade das Informações: garantir que as informações sejam utilizadas exclusivamente para os fins para os quais foram coletadas, condicionando o acesso à devida autorização.

7.7. Procedimentos de Segurança: implementar e manter controles para reduzir vulnerabilidades, incluindo:

- (i) considerar como sensíveis, no mínimo, os dados cadastrais e demais informações que permitem a identificação de clientes;
- (ii) autenticação e criptografia;
- (iii) prevenção e detecção de intrusão;
- (iv) prevenção de vazamento de informações;
- (v) testes periódicos e varreduras para identificar vulnerabilidades;

- (vi) proteção contra *softwares* maliciosos;
- (vii) rastreabilidade de informações e controle de acessos;
- (viii) segmentação da rede de computadores;
- (ix) manutenção de backups de dados e informações.

7.8. Segurança das Informações Sensíveis: garantir controles específicos para proteger e rastrear informações sensíveis, minimizando riscos ao mais alto nível possível.

7.9. Gerenciamento Integrada de Incidentes:

- (i) registrar, analisar causas e impactos de incidentes;
- (ii) estabelecer parâmetros para avaliação da relevância e implicações;
- (iii) controlar efeitos de incidentes, incluindo aqueles reportados por terceiros; e
- (iv) promover o compartilhamento de informações sobre incidentes relevantes com outras instituições autorizadas pelo BCB.

7.10. Reportes de Riscos: qualquer risco identificado em relação às informações deverá ser imediatamente comunicado pelo Colaborador através do e-mail seguranca@dillon.com.br.

7.11. Continuidade de Negócios: elaborar cenários de incidentes e considerá-los em testes de continuidade de negócios dos serviços de pagamento prestados pela instituição.

7.12. Fornecedores e Parceiros: a Dillon DTVM não permite acesso a seu ambiente tecnológico a fornecedores e parceiros exceto os contratados especificamente para tanto ou que necessitam de acesso específico. Nesses casos, credenciais de login e senha específicos serão fornecidos a estes terceiros, com acesso limitado às informações que necessitam para a execução dos serviços para os quais foram contratados, bem como com monitoramento constante pelo Responsável por Segurança Cibernética da Dillon DTVM.

7.12.1. Caso o Responsável por Segurança Cibernética da Dillon DTVM identifique qualquer tipo de ameaça ou suspeita de uso indevido das credenciais de/por fornecedores e parceiros, o acesso poderá ser imediatamente suspenso para averiguação interna, cabendo ao Comitê de Segurança da Informação e Segurança Cibernética a decisão sobre o reestabelecimento – ou não – conforme a conclusão da análise.

7.13. Gerenciamento desta Política:

- (i) monitoramento contínuo do cumprimento;
- (ii) implementação de melhorias nos processos de segurança; e
- (iii) atualização anual e revisões extraordinárias conforme evolução das ameaças

cibernéticas e alterações regulatórias sobre o tema.

7.14. Divulgação:

(i) Divulgação interna:

- a. compartilhamento integral com funcionários;
- b. inclusão nos contratos com prestadores de serviços terceirizados; e
- c. envio de atualizações anuais via e-mail corporativo;

(ii) Divulgação externa:

- a. publicação das diretrizes principais em seu website institucional; e
- b. disponibilização do resumo da política ao público geral.

8. PAPÉIS E RESPONSABILIDADES DAS ÁREAS ENVOLVIDAS

8.1. Todos os Colaboradores dentro de suas atividades têm funções e responsabilidades relacionadas à Segurança da Informação e Segurança Cibernética.

8.1.1. Diretoria Executiva: a Diretoria é responsável por assegurar a Segurança da Informação e Segurança Cibernética.

8.1.1.1. Dentre as principais responsabilidades, destacam-se:

- (i) avaliar, aprovar e revisar periodicamente esta presente Política, incluindo suas atualizações, garantindo alinhamento com as melhores práticas e regulamentações aplicáveis; e
- (ii) assegurar a implementação e o cumprimento integral desta Política em todas as atividades da Dillon DTVM, promovendo a adesão por parte de Colaboradores, Parceiros e Fornecedores.

8.1.2. Comitê de Segurança da Informação e Segurança Cibernética ou Comitê de Riscos ou Comitê de Compliance: é responsável por analisar e decidir quaisquer demandas submetidas. É composto pelo Diretor Presidente, Diretor de Riscos e Compliance, Diretor responsável pela Tecnologia da Informação e poderá contar com Colaboradores de Riscos, Tecnologia da Informação, Compliance e Backoffice, de acordo com a pertinência.

8.1.2.1. As reuniões do Comitê de Segurança da Informação e Segurança Cibernética ou Comitê de Riscos ou Comitê de Compliance ocorrem, ao menos, anualmente, podendo suas deliberações serem realizadas de forma não presencial, formalizadas por e-mail.

8.1.2.2. Dentre as principais responsabilidades, destacam-se:

- (i) submeter os relatórios anuais de implementação do Plano de Ação e de Resposta a Incidentes e o relatório final sobre incidentes ao Comitê de Segurança da Informação e Segurança Cibernética ou Comitê de Riscos ou Comitê de Compliance, quando existente, na sua inexistência, à diretoria da instituição, para análise crítica e recomendações de aprimoramento;
- (ii) garantir que o relatório em conformidade com a Resolução CMN nº 4.893/2021 seja apresentado ao Conselho de Administração ou, na sua inexistência, à Diretoria da Dillon DTVM até o dia 31 de março do ano subsequente à data-base, proporcionando visibilidade e acompanhamento adequado das ações realizadas; e
- (iii) garantir que o relatório em conformidade com a Resolução CVM nº 35/2021 seja apresentado ao Conselho de Administração ou, na sua inexistência, à Diretoria da Dillon DTVM até o último dia do mês de abril do ano subsequente à data-base, proporcionando visibilidade e acompanhamento adequado das ações realizadas.

8.1.3. Diretor responsável de Segurança da Informação e Segurança Cibernética: Representa a Dillon DTVM perante o Banco Central do Brasil como Diretor responsável pelo cumprimento das obrigações previstas nas Resoluções CMN nº 4.893/2021 e CVM nº 35/2021 ou normativo equivalente.

8.1.3.1. Dentre as principais responsabilidades, destacam-se:

- (iv) implementar e manter esta Política, formulada com base em princípios e diretrizes robustas, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Dillon DTVM;
- (v) elaborar e apresentar anualmente o relatório detalhado sobre a implementação do Plano de Ação e de Resposta a Incidentes, abordando as ações executadas, os resultados obtidos, os desafios enfrentados e as lições aprendidas, com foco na melhoria contínua da segurança da informação, e apresentar ao Conselho de Administração ou, na sua inexistência, à Diretoria da Dillon DTVM até o dia 31 de março do ano subsequente à data-base, garantindo a visibilidade e o acompanhamento adequado das ações implementadas;

- (vi) elaborar e enviar à SMI o relatório final sobre incidentes de segurança cibernética;
- (vii) garantir a execução eficaz do Plano de Ação e de Resposta a Incidentes, coordenando as ações necessárias para mitigar riscos, resolver incidentes de segurança e implementar melhorias contínuas nos processos de Segurança Cibernética;
- (viii) monitorar e gerenciar indicadores relacionados à Segurança da Informação e Segurança Cibernética, identificados nos processos de monitoramento contínuo e reportados pela Área de Tecnologia da Informação ou pelos Colaboradores, garantindo a análise, acompanhamento e comunicação eficaz para suportar a tomada de decisões, mitigação de riscos e aprimoramento dos controles de segurança;
- (ix) implantar e monitorar processos de segurança cibernética, com a implementação de medidas para eliminar ou mitigar riscos relacionados a sistemas de informação e segurança cibernética;
- (x) realizar tratamento de riscos e vulnerabilidades em ativos e processos, identificando e corrigindo falhas para garantir a proteção das informações e a integridade dos sistemas;
- (xi) informar imediatamente a alta direção sobre incidentes de segurança, comunicando falhas, violações ou anomalias que possam comprometer a segurança dos ativos e das informações da Dillon DTVM;
- (xii) promover a adoção e coordenação de boas práticas em Segurança da Informação e Segurança Cibernética, identificando e implementando melhorias contínuas nos controles e processos para fortalecer a proteção contra riscos e alinhar as operações às melhores práticas de mercado;
- (xiii) manter a infraestrutura tecnológica atualizada, seguindo as recomendações dos fabricantes e as melhores práticas de mercado, para garantir a resiliência e segurança dos sistemas;
- (xiv) gerenciar acessos aos sistemas e informações, controlando rigorosamente os acessos para garantir que apenas usuários autorizados tenham acesso conforme suas funções e responsabilidades;

- (xv) garantir a continuidade dos negócios, implementando planos e estratégias que assegurem a recuperação rápida das operações críticas em caso de incidentes de segurança;
- (xvi) proteger ambientes tecnológicos e suas contingências, adotando medidas de segurança para proteger todos os ambientes tecnológicos e garantir planos de ação ou contingência eficazes;
- (xvii) controlar o acesso físico às instalações, monitorando e restringindo o acesso às áreas sensíveis e recursos da Dillon DTVM, garantindo a segurança física dos ativos; e
- (xviii) promover treinamentos contínuos em Segurança da Informação e Segurança Cibernética para todos os Colaboradores, Fornecedores e Parceiros, reforçando a conscientização sobre a importância da segurança e as boas práticas no uso de sistemas e dados.

8.1.4. Diretor de Controles Internos: é responsável pelo cumprimento das obrigações previstas na Resolução CVM nº 35/2021 ou normativo equivalente.

8.1.4.1. Dentre as principais responsabilidades, destacam-se:

- (i) deve encaminhar, até o último dia útil de abril de cada ano, um relatório detalhado à Diretoria da Dillon DTVM, contendo: controles internos implantados, metodologia aplicada, procedimentos para análise de deficiências, testes realizados, monitoramento, recomendações sobre as deficiências, avaliação dos riscos.

8.1.5. Área de Compliance: Tem como principais atribuições:

- (i) identificar, avaliar e acompanhar as principais regulamentações e normas aplicáveis à Segurança da Informação e Segurança Cibernética, propondo e implementando, quando aprovado, medidas corretivas para mitigar riscos e garantir conformidade;
- (ii) analisar e executar ações necessárias para assegurar o cumprimento desta Política, alinhando as práticas organizacionais aos seus objetivos e diretrizes;
- (iii) fornecer suporte técnico e estratégico às demais áreas da organização, promovendo a adoção de padrões e boas práticas em Segurança da Informação e Segurança Cibernética;

- (iv) apoiar a área de Segurança da Informação e Segurança Cibernética na realização de treinamentos e campanhas de conscientização, disseminando internamente os conceitos e princípios desta Política;
- (v) acompanhar e participar ativamente do processo de revisão e atualização desta Política, garantindo que ela permaneça alinhada às necessidades organizacionais, regulamentações vigentes e avanços tecnológicos; e
- (vi) garantir o compartilhamento das atualizações desta Política de Segurança da Informação e Segurança Cibernética com todos os envolvidos na Dillon DTVM, incluindo Clientes, Colaboradores, Fornecedores, Parceiros, Partes Interessadas e a própria instituição.

8.1.6. Gestores das Demais Áreas: Tem como principais atribuições:

- (i) assegurar que todos os Colaboradores tenham amplo acesso à Política de Segurança da Informação e Segurança Cibernética, promovendo sua compreensão e aplicação no dia a dia;
- (ii) realizar avaliações periódicas do nível de sigilo e segurança requerido para a proteção das informações sob sua responsabilidade e da equipe, garantindo a implementação de controles adequados;
- (iii) designar múltiplos responsáveis para processos e operações suscetíveis a fraudes, assegurando a segregação de funções e mitigando riscos operacionais;
- (iv) acionar as áreas responsáveis para a aplicação de penalidades cabíveis aos Colaboradores que descumprirem a Política de Segurança da Informação e Segurança Cibernética, em conformidade com as normas internas e legais; e
- (v) autorizar os acessos de Colaboradores apenas quando estritamente necessários, seguindo os princípios de privilégio mínimo e garantindo que os acessos estejam alinhados às funções e responsabilidades.

8.1.7. Colaboradores:

- (i) é responsabilidade dos Colaboradores ler, compreender e cumprir integralmente os termos desta Política da Dillon DTVM;

- (ii) encaminhar à Área de Tecnologia da Informação quaisquer dúvidas ou solicitações de esclarecimento relacionadas a esta Política;
- (iii) notificar imediatamente a Área de Tecnologia da Informação sobre qualquer evento que viole esta Política ou que comprometa, ou possa vir a comprometer, a segurança das informações ou dos recursos computacionais da Dillon DTVM; e
- (iv) assumir responsabilidade por eventuais descumprimentos desta Política, conforme estabelecido no capítulo Sanções e Punições.

8.1.8. Fornecedores e Parceiros:

- (i) cumprir integralmente as determinações desta Política e dos Procedimentos de Tecnologia da Informação publicados pela Dillon DTVM, garantindo a adesão às diretrizes estabelecidas; e
- (ii) apresentar os documentos de Políticas e Procedimentos da Dillon DTVM a todos os Colaboradores das empresas Fornecedoras ou Parceiras, assegurando o cumprimento das determinações contidas nesses documentos.

9. GERENCIAMENTO DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

9.1. Para garantir o cumprimento das diretrizes mencionadas e a aderência aos princípios de Segurança da Informação e Segurança Cibernética, a Dillon DTVM adota os processos descritos a seguir.

10. GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

10.1. Gerenciamento de Ativos:

10.1.1. Os Ativos são inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. O acesso às salas com armazenagem de documentos físicos é restrito e limitado, por meio de mecanismos de autenticação e autorização de acesso, ao Diretor de Riscos e Compliance, bem como ao Diretor de Tecnologia e Segurança da Informação.

10.1.2. Os Ativos devem ser utilizados exclusivamente para a finalidade autorizada. A Dillon DTVM assegurará proteção aos Ativos durante todo seu

ciclo de vida, garantindo os princípios da autenticidade, confidencialidade, disponibilidade e integridade.

10.1.3. A Dillon DTVM considera como sensíveis, no mínimo, os dados cadastrais e demais informações que permitem a identificação de clientes (de acordo com a Lei nº 13.709/2018), suas operações, posições de custódia e quaisquer outros dados (especialmente os financeiros) relacionados aos clientes e Colaboradores.

10.2. Autenticação:

10.2.1. A Dillon DTVM, através de concessão de credenciais de acesso, adota mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados (ou seja, que necessitem das informações ali contidas para a execução das atividades para as quais foram contratados), considerando o princípio do menor privilégio, a segregação de funções e a classificação da informação.

10.3. Segmentação de Rede:

10.3.1. A Dillon DTVM segmenta a sua rede, concedendo acesso segregado aos Colaboradores e a terceiros, mediante credenciais distintas de acesso. Isso significa que visitantes e clientes terão acesso a uma rede segregada que não é vinculada à interna da Dillon DTVM, evitando, assim, a exposição de seus arquivos e informações. O acesso a terceiros é individual e se modifica a cada login, de modo que mesmo que o visitante compareça mais vezes ao escritório, a cada acesso, ele precisará atualizar as suas credenciais para ingressar na internet.

10.3.2. Somente o Departamento de Tecnologia e Segurança da Informação possui ingerência para criar, alterar ou excluir regras nos firewalls e ativos de rede.

10.4. Classificação da Informação:

10.4.1. As informações são classificadas segundo sua criticidade e sensibilidade para o negócio e seus Clientes:

- (i) informação pública: acessível por todos, sem restrição (ex: dados divulgados ao mercado e dados promocionais);
- (ii) informação interna: acessível somente por Colaboradores da Dillon DTVM (ex: normas, procedimentos e formulários);

- (iii) informação restrita: acessível somente por Colaboradores que necessitam para suas atribuições (ex: contratos e documentos estratégicos); e
- (iv) informação confidencial: trata-se de uma informação crítica para a Dillon DTVM ou seus Clientes, cuja divulgação não autorizada pode gerar impactos financeiros, reputacionais, operacionais e até sanções administrativas, civis ou criminais. Acessível somente por Colaboradores com permissão específica (ex: plano estratégico e informações de clientes).

10.4.2. Quando de sua circulação, estas informações deverão ser identificadas conforme a sua classificação, de modo que o seu destinatário saiba especialmente quando se tratar de informações confidenciais.

10.5. Sigilo de Informações Privilegiadas:

10.5.1. Colaboradores com acesso a informações privilegiadas devem manter sigilo total e estão proibidos de negociar ou compartilhar tais dados antes da divulgação oficial.

10.5.2. São consideradas informações privilegiadas:

- (i) informações objeto de sigilo por força contratual; e
- (ii) informações de caráter estratégico.

10.5.3. Apenas Colaboradores autorizados podem se manifestar publicamente, fornecendo informações transparentes e completas, visando os interesses da instituição.

10.5.4. As informações e dados nos sistemas da Dillon DTVM são de sua propriedade exclusiva.

10.5.5. Os direitos sobre know-how e confidencialidade persistem após o desligamento dos Colaboradores.

10.6. Controle e Monitoramento de Acessos:

10.6.1. A Dillon DTVM adota controles e monitoramento em toda infraestrutura para prevenir e detectar acessos não autorizados aos ambientes segregados, sistemas internos e informações restritas, através da autenticação de usuários, segregação de funções, rastreabilidade e aprovação de acessos.

10.6.2. O monitoramento proativo e periódico do acesso e uso dos recursos físicos e tecnológicos, incluindo ambientes, sistemas e equipamentos, permite identificar ações indesejadas ou não autorizadas.

10.7. Gerenciamento de Senha:

10.7.1. A Dillon DTVM fornece credenciais de acesso aos Colaboradores e terceiros quando de seu ingresso, solicitando que a senha seja imediatamente trocada quando do primeiro uso.

10.7.2. Quando de seu fornecimento e através de suas políticas internas, a Dillon DTVM reforça que as senhas são confidenciais, pessoais e intransferíveis, devendo conter, no mínimo, oito caracteres, uma letra maiúscula, uma minúscula, um número e um caracter especial.

10.7.3. Nada obstante, os Colaboradores e terceiros são instados a atualizar as suas senhas de acesso, pelo menos, a cada 3 (três) meses, sob pena de terem os seus acessos bloqueados até que o façam.

10.8. Gerenciamento de Riscos e Segurança:

10.8.1. A Dillon DTVM mantém processo estruturado para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação, permitindo a adoção de medidas mitigatórias adequadas em caso de incidentes.

10.8.2. O processo de Gerenciamento de Riscos e Segurança abrange:

- (i) levantamento dos impactos organizacionais: identificação das áreas impactadas direta e indiretamente;
- (ii) priorização de mudanças: avaliação e classificação das alterações necessárias no ambiente tecnológico;
- (iii) planejamento: definição dos planos de implementação e correções, visando maximizar a segurança e minimizar riscos;
- (iv) monitoramento contínuo: realização de testes de varredura para detectar vulnerabilidades, avaliar riscos e implementar medidas corretivas;
- (v) mobilização: coordenação entre Diretor responsável de Segurança da Informação e Segurança Cibernética, Comitê de Segurança da Informação e Segurança Cibernética e ao Comitê de Compliance para direcionar as ações necessárias;
- (vi) comunicação: divulgação dos objetivos e desenvolvimento do plano de comunicação para engajamento dos Colaboradores;
- (vii) treinamento: capacitação contínua dos envolvidos no processo de Gerenciamento de Riscos e controles do ambiente tecnológico; e
- (viii) atualização periódica: manutenção da infraestrutura tecnológica para prevenir vulnerabilidades e brechas de segurança contra-ataques de vírus e outros *softwares* maliciosos.

10.9. Gerenciamento de Fornecedores e Parceiros:

10.9.1. A Dillon DTVM avalia o nível de maturidade dos controles de Segurança da Informação e Segurança Cibernética de seus prestadores de serviços, Fornecedores, e Parceiros que processam e armazenam seus dados, analisando seus planos de tratamento de incidentes.

10.9.2. A instituição disponibiliza o canal seguranca@dillon.com.br para que Fornecedores e Parceiros reportem incidentes de Segurança da Informação e Segurança Cibernética relacionados às suas informações e diretrizes desta Política.

10.10. Segurança Física do Ambiente:

10.10.1. A Dillon DTVM possui um sistema de controle de acesso para Colaboradores, Fornecedores e Parceiros em áreas restritas, mediante a leitura de cartões que são entregues a quem necessita de acesso.

10.10.2. Estes cartões são registrados no nome de seus portadores e seu uso é intransferível.

10.10.3. Para acesso de terceiros não autorizados a áreas internas da Dillon DTVM, a autorização do Diretor de Riscos e Compliance deverá ser previamente obtida ou, então, deverá este acompanhar o visitante. Na falta deste, poderá o CEO da Dillon DTVM acompanhar, dando ciência ao Diretor de Riscos e Compliance acerca do acesso. Sob nenhuma hipótese, o visitante deverá circular desacompanhado nas dependências da Dillon DTVM.

10.10.2. Equipamentos e instalações que processam informações críticas ou sensíveis, bem como o servidor da Dillon DTVM, são mantidos em áreas seguras, com controles de acesso e proteção contra ameaças físicas e ambientais.

10.11. Aquisição, Desenvolvimento e Manutenção de Sistemas:

10.11.1. Todos os sistemas da Dillon DTVM, adquiridos ou desenvolvidos internamente, passam por Avaliação de Riscos antes da implementação, assegurando alinhamento com as práticas de Segurança da Informação desta Política.

10.11.2. As alterações nos sistemas seguem o processo de gerenciamento de mudanças, incluindo:

- (i) remoção de todos os dados de teste (contas, usuários, senhas) antes da implementação;
- (ii) proteção da confidencialidade dos dados pessoais e corporativos através de técnicas de anonimização, pseudonimização, reidentificação ou limpeza;
- (iii) capacitação dos desenvolvedores em práticas de codificação segura;
- (iv) separação clara entre equipes de desenvolvimento/testes e manutenção do ambiente de produção; e
- (v) segregação dos ambientes de teste, desenvolvimento e produção.

10.12. Destruição e Descarte de Ativos de Informações:

10.12.1. A Dillon DTVM realiza o descarte seguro de ativos de informações em todos os dispositivos que os armazenam, incluindo notebooks, servidores, mídias removíveis, documentos físicos e demais meios.

10.13. Cópia de Segurança (*Backup*) e Registro de Eventos (*Logs*):

10.13.1. A Dillon DTVM mantém uma rotina sistemática de *backup* e restauração de dados para garantir a disponibilidade das informações essenciais às suas operações. As cópias de segurança são realizadas em intervalos regulares e armazenadas em ambientes seguros, separados dos sistemas originais, garantindo proteção contra falhas, desastres ou ataques.

10.13.2. Os *backups* são regularmente testados em equipamentos distintos do ambiente de produção, assegurando a integridade dos dados. A Dillon DTVM realiza o registro de *logs* que permitem rastrear acessos, identificando usuário, data, meio de acesso e informações consultadas. Todos os *logs* são protegidos contra modificações e acessos não autorizados.

10.13.3. As diretrizes adicionais sobre Cópias de Segurança podem ser consultadas no Procedimento da Área de TI para Cópias de Segurança (*Backup*).

10.14. Proteção contra Vírus, Arquivos e *Softwares* Maliciosos:

10.14.1. A Dillon DTVM implementa mecanismos de proteção contra vírus e outras ameaças digitais (como *phishing* e *spam*) para evitar sua propagação em computadores, sistemas e servidores internos, reduzindo vulnerabilidades. Todos os computadores da rede interna devem manter *softwares* de segurança, incluindo antivírus, devidamente instalados e atualizados.

10.15. Criptografia:

10.15.1. Os ativos de informação da Dillon DTVM devem utilizar criptografia apropriada, conforme sua classificação, em todas as transmissões realizadas em redes públicas. Isso assegura a proteção durante todo o ciclo de vida da informação, em conformidade com os padrões de segurança estabelecidos pelos órgãos reguladores.

10.16. Testes de Penetração (Pentest):

10.16.1. Em conformidade com o parágrafo 2º do Art. 3º da Resolução CMN nº 4.893/2021, a Dillon DTVM realiza testes de penetração semestrais para prevenir e detectar intrusões, evitar vazamentos de informações, identificar vulnerabilidades, proteger contra *softwares* maliciosos e verificar mecanismos de rastreabilidade.

10.17. Avaliação Periódica:

10.17.1. A Dillon DTVM avalia regularmente suas práticas de Segurança da Informação e Segurança Cibernética para garantir a conformidade das ações de seus Colaboradores com esta Política e com as exigências legais e regulatórias.

10.17.2. Os documentos e procedimentos relacionados à Segurança da Informação e Segurança Cibernética são revisados periodicamente, considerando análises críticas, requisitos legais, estatutários, regulamentares e contratuais que possam impactar os processos de segurança.

10.18. Troca de Informações:

10.18.1. Na Dillon DTVM, a transmissão de informações digitais por canais não seguros requer análise prévia conforme o nível de classificação da informação, avaliando a necessidade de criptografia. Para transmissão física de dados digitais, deve-se analisar a necessidade de rótulos, lacres, assinaturas e criptografia, de acordo com a classificação da informação.

10.18.2. As comunicações com redes de fornecedores e parceiros devem sempre utilizar criptografia ou outros mecanismos que garantam proteção, confidencialidade e integridade.

10.18.3. As áreas de negócio devem sempre utilizar canais de comunicação seguros (SFTP, SSH, TLS) para trocar informações sensíveis com Fornecedores e Parceiros. Quando não for possível, as informações devem ser protegidas com criptografia ou senha forte para prevenir vazamentos.

10.19. Plano de Continuidade de Negócios:

10.19.1. A Dillon DTVM mantém um plano de continuidade de serviços baseado em estratégias preventivas e planos de ação para identificar e preservar serviços essenciais durante contingências. Sua infraestrutura é suportada em *Cloud*, não utilizando recursos físicos para manter ou atualizar serviços essenciais e informações dos usuários e transações.

10.19.2. A Dillon DTVM realiza:

- (i) mapeamento de processos críticos;
- (ii) análise de impacto nos negócios;
- (iii) inventário de cenários de crises cibernéticas;
- (iv) testes periódicos de continuidade dos serviços em ambiente controlado;
- e
- (v) definição de procedimentos e controles para prevenção e tratamento de incidentes por Fornecedores e Parceiros.

10.19.3. A infraestrutura física da Dillon DTVM consiste em equipamentos em rede para manutenção e distribuição dos links de internet, e testes de contingência são realizados periodicamente para garantir a Continuidade dos Negócios da instituição.

11. GERENCIAMENTO DA SEGURANÇA CIBERNÉTICA

11.1. Incidentes de Segurança:

11.1.1. A Dillon DTVM estabelece processos para identificação, tratamento e registro de incidentes de segurança, visando mitigar riscos e preservar a integridade, confidencialidade e disponibilidade das informações, em conformidade com as Resoluções CMN nº 4.893/2021 e CVM nº 35/2021.

11.2. Classificação de Relevância dos Incidentes:

11.2.1. A Dillon DTVM classifica os incidentes de segurança segundo sua relevância, classificação das informações envolvidas e impacto na continuidade dos negócios, conforme detalhado em manuais específicos.

11.3. Gerenciamento de Incidentes:

11.3.1. Incidentes ou suspeitas identificados por Colaboradores, Parceiros ou Fornecedores devem ser imediatamente comunicados via e-mail

seguranca@dillon.com.br. Os incidentes são classificados pelo risco e impacto nos negócios, sendo registrados, tratados e comunicados adequadamente.

11.3.2. A Dillon DTVM adota procedimentos para mitigar efeitos de incidentes relevantes e interrupções nos serviços de processamento, armazenamento de dados e computação em nuvem.

11.4. Compartilhamento de Informações:

11.4.1. A Dillon DTVM compartilha informações sobre incidentes relevantes com instituições autorizadas pelo BCB, respeitando sigilo e livre concorrência. Em caso de incidentes relevantes ou interrupções, comunica o BCB e implementa medidas para reinício das atividades, documentando critérios da situação de crise, conforme estabelece o seu Plano de Continuidade de Negócios.

11.4.2. A Dillon DTVM reporta tempestivamente à SMI e aos administradores a ocorrência de incidentes relevantes que afetem seus sistemas críticos e causem impacto significativo aos clientes, conforme disposto no § 1º do Art. X da Resolução CVM nº 35/2021.

11.4.3. Essa comunicação inclui:

- (i) a descrição do incidente, indicando como os clientes foram afetados;
- (ii) avaliação do número de clientes potencialmente impactados;
- (iii) as medidas já adotadas ou que se pretende adotar;
- (iv) o tempo consumido na solução do evento ou o prazo esperado para a resolução; e
- (v) qualquer outra informação considerada importante, conforme § 2º do mesmo artigo.

11.5. Plano de Ação e Resposta a Incidentes:

11.5.1. O Plano de Ação da Dillon DTVM abrange:

- (i) ações para adequar estruturas organizacional e operacional conforme esta Política;
- (ii) rotinas, procedimentos, controles e tecnologias para prevenção e resposta a incidentes;
- (iii) área responsável pelo registro e controle dos efeitos de incidentes relevantes; e
- (iv) diretor designado responsável pela presente Política e execução deste Plano de Ação.

11.5.3. O Plano de Ação e de Resposta a Incidentes deve ser submetido ao Comitê de Segurança da Informação e Segurança Cibernética ou Comitê de Riscos, quando existente e é aprovado pelo conselho de administração ou diretoria, documentado, e revisado anualmente.

11.6. Relatório Anual de Resposta a Incidentes:

11.6.1. O Relatório Anual de Resposta a Incidentes é elaborado com data-base de 31 de dezembro, incluindo:

- (i) efetividade das ações de adequação organizacional e operacional;
- (ii) resultados da implementação de controles e tecnologias na prevenção e na resposta a incidentes;
- (iii) incidentes ocorridos e relevantes do período relacionados ao ambiente cibernético; e
- (iv) resultados dos testes de continuidade dos serviços prestados e intermediação de operações, considerando cenários de indisponibilidade ocasionada por incidentes.

11.6.2. O Relatório Anual de Resposta a Incidentes é:

- (i) submetido ao Comitê de Segurança da Informação e Segurança Cibernética ou ao Comitê de Riscos, quando existente;
- (ii) apresentado aos Administradores até 31 de março do ano seguinte, conforme a Resolução CMN nº 4.893/2021; e
- (iii) revisado anualmente.

11.6.3. A Dillon DTVM elabora e envia à SMI o relatório final sobre incidentes contendo:

- (i) descrição do incidente e das medidas tomadas, informando o impacto gerado pelo incidente sobre a operação da instituição e seus reflexos sobre os dados dos clientes; e
- (ii) aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de incidentes de segurança cibernética, se for o caso.

11.6.4. A Dillon DTVM mantém à disposição da SMI cópia:

- (i) das comunicações realizadas com seus clientes, se houver;
- (ii) dos relatórios internos de investigação produzidos pelo intermediário ou por terceiros sobre a análise do incidente e as conclusões dos exames efetuados; e
- (iii) os documentos são mantidos pelo prazo mínimo de 5 (cinco) anos ou por prazo

superior, conforme determinação expressa da CVM.

11.7. Relatório Anual de Controles Internos:

11.7.1. O Diretor de Controles Internos deve encaminhar, até o último dia útil de abril de cada ano, um relatório detalhado à Diretoria da Dillon DTVM do intermediário, contemplando os seguintes pontos:

(i) Descrição detalhada e atualizada:

- a) controles internos implantados, com informações sobre os tipos de controles existentes e as atividades e operações abrangidas;
- b) metodologia aplicada para realização de exames, como mecanismos de monitoramento e critérios de seleção de amostras; e
- c) procedimentos para análise de deficiências identificadas.

(ii) Detalhamento dos testes e conclusões:

- a) testes realizados para verificar eficiência dos controles nas atividades descritas na Resolução CVM nº 35/2021, como cadastro de clientes, transmissão de ordens e segurança cibernética; e
- b) monitoramento da infraestrutura de tecnologia da informação, incluindo o programa de segurança cibernética.

(iii) Recomendações sobre deficiências:

- a) identificação de deficiências apontadas no período de referência e nos relatórios anteriores, com propostas de planos de ação e cronogramas de correção.

(iv) Avaliação de riscos:

- a. riscos relacionados aos controles internos e vulnerabilidades a ataques cibernéticos.

(v) Manifestação do diretor responsável:

- a. avaliação das deficiências encontradas, andamento das ações para saná-las, adequação do plano de continuidade de negócios e evolução do cumprimento das normas regulatórias;
- b. informar sobre a evolução das ações planejadas para sanar deficiências identificadas no exercício anterior, incluindo as identificadas pela CVM, pela entidade administradora do mercado e pela entidade autorreguladora;

- c. especificar, em relação às deficiências apontadas nos relatórios anteriores, se os cronogramas de saneamento foram implementados e apresentar os resultados das ações adotadas para corrigir essas deficiências;
- d. avaliar a evolução do intermediário no cumprimento das exigências regulatórias durante o período de competência do relatório; e
- e. indicar a adequação do plano de continuidade de negócios, destacando eventuais necessidades de aperfeiçoamento.

11.8. Mecanismos de Rastreabilidade e Controle:

11.8.1. A Dillon DTVM adota mecanismos de rastreabilidade e controles específicos para garantir a segurança das informações sensíveis, incluindo:

- (i) controles de rastreabilidade para todas as operações e transações realizadas nos sistemas;
- (ii) gerenciamento específico de informações sensíveis envolvidas durante os processos;
- (iii) controles alinhados com a LGPD (Lei 13.709/2018);
- (iv) registro e monitoramento de acessos e alterações em dados sensíveis; e
- (v) trilhas de auditoria para operações críticas.

11.8.2. A rastreabilidade deve permitir a identificação da origem, alterações realizadas e responsáveis por cada operação que envolva informações sensíveis.

11.9. Registro e Análise de Incidentes:

11.9.1. A Dillon DTVM mantém processo estruturado de documentação e análise de incidentes, que inclui:

- (i) registro detalhado dos incidentes relevantes;
- (ii) análise de causa raiz e impacto nos negócios;
- (iii) avaliação dos efeitos nas atividades da instituição;
- (iv) monitoramento das ações corretivas e preventivas;
- (v) integração de informações de incidentes reportados por fornecedores e parceiros;
- (vi) documentação das medidas tomadas para resolução;
- (vii) métricas de impacto operacional e financeiro; e
- (viii) lições aprendidas para prevenção futura.

11.9.2. O processo visa garantir aprendizado contínuo e aprimoramento dos controles de segurança.

11.10. Treinamentos e Conscientização em Segurança:

11.10.1. A Dillon DTVM desenvolve e mantém programa abrangente de conscientização em segurança que inclui:

- (i) treinamentos regulares e obrigatórios sobre Segurança da Informação e Cibernética;
- (ii) campanhas de conscientização com simulações práticas de ameaças;
- (iii) avaliações periódicas de conhecimento e efetividade dos treinamentos;
- (iv) comunicação clara sobre riscos e melhores práticas de segurança;
- (v) orientação específica por função e nível de acesso às informações;
- (vi) guias práticos de segurança para usuários finais; e
- (vii) atualizações sobre novas ameaças e medidas preventivas.

11.10.2. Os Administradores lideram pelo exemplo, promovendo cultura de segurança e melhoria contínua dos controles e processos. O programa é regularmente atualizado para abordar novos riscos e requisitos regulatórios.

11.11. Segurança em Novos Produtos e Serviços:

11.11.1. A Dillon DTVM avalia os riscos cibernéticos em:

- (i) operacionalização em novas operações;
- (ii) mudanças significativas em processos existentes;
- (iii) implementação de novas tecnologias; e
- (iv) alterações em sistemas críticos.

11.11.2. Cada mudança passa por avaliação de segurança e testes antes da implementação, garantindo que controles adequados sejam estabelecidos para proteger Clientes e dados.

12. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E COMPUTAÇÃO NA NUVEM

12.1. A Dillon DTVM não tem planos de contratação de serviços de processamento, armazenamento de dados e computação em nuvem, a curto ou médio prazos.

12.2. Caso haja a necessidade de contratação futura destes serviços, a Dillon DTVM observará a plena conformidade à Resolução CMN nº 4.893/2021.

13. CONTRATAÇÃO DE SERVIÇOS RELEVANTES PRESTADOS POR TERCEIROS

13.1. A Dillon DTVM realiza a identificação e classificação de prestadores de serviços relevantes, avaliando regularmente os controles de segurança implementados por esses provedores.

13.2. Os contratos firmados com terceiros incluem cláusulas que asseguram a confidencialidade, integridade, disponibilidade e recuperação dos dados e informações processados ou armazenados.

13.3. A Dillon DTVM exige que os contratos garantam seu pleno acesso aos dados e informações sob responsabilidade dos Fornecedores e Parceiros, assegurando sua capacidade de monitorar e auditar processos críticos.

13.4. Conforme a Resolução CVM nº 35, Art. 48, mesmo com a terceirização, a instituição mantém a responsabilidade integral pelo registro e arquivamento dos documentos e informações.

13.5. A Dillon DTVM assegura que os contratos com terceiros não contenham cláusulas que limitem ou impeçam o acesso da CVM e de entidades autorreguladoras aos contratos, documentos e informações processadas pelos provedores.

13.6. Auditorias periódicas são realizadas nos prestadores de serviços, para verificar o cumprimento das obrigações contratuais e regulamentares, especialmente no que se refere à proteção dos dados e à disponibilidade das informações.

13.7. A Dillon DTVM implementa Plano de Ação e Resposta à Incidentes, para lidar com interrupções ou incidentes envolvendo os dados processados por terceiros, garantindo a continuidade dos serviços.

14. SANÇÕES ADMINISTRATIVAS

14.1. As violações desta Política, incluindo omissões ou tentativas não consumadas, que exponham a Dillon DTVM a riscos com repercussões reputacionais, sociais, políticas ou econômicas, estarão sujeitas a penalidades como advertência por escrito, suspensão não remunerada, demissão por justa causa e/ou ação judicial.

14.2. O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato e à Diretoria.

14.3. No caso de Colaboradores temporários ou terceiros, o Comitê ou a Diretoria Executiva analisará a ocorrência e deliberará sobre as sanções e punições aplicáveis, conforme os termos previstos no contrato.



Diretoria: 04 Compliance e Riscos
Área: 01 Compliance
Título: 01 CODIGO PSIC

Publicação: 05/2024
Atualização: 05/11/2025
Versão: 004

15. DECLARAÇÃO DE RESPONSABILIDADE

15.1. Os Colaboradores da Dillon DTVM devem aderir formalmente a esta Política por meio de um termo de compromisso, no qual se comprometem a agir em conformidade com suas diretrizes.

15.2. Os contratos firmados pela Dillon DTVM com fornecedores que envolvam ativos de informação relacionados a esta Política devem conter uma cláusula que assegure a proteção e a segurança das informações.

16. DIVULGAÇÃO DESTA POLÍTICA

16.1. A Dillon DTVM disponibiliza em sua página na internet orientações claras aos seus clientes sobre suas principais práticas de segurança da informação, incluindo controles de acesso lógico aplicados aos clientes, proteção da confidencialidade de dados sensíveis e medidas preventivas que os clientes devem adotar para garantir a segurança cibernética ao acessar os sistemas fornecidos pela instituição.

16.2. Esta Política será divulgada a todos os Colaboradores da Dillon DTVM e empresas terceirizadas desde o início do relacionamento contratual, com atualizações anuais compartilhadas por e-mail.

16.3. A Dillon DTVM disponibilizará em seu site institucional um resumo ao público contendo as diretrizes principais desta Política.

17. VIGÊNCIA E APROVAÇÃO DESTA POLÍTICA

17.1. Esta política será revisada anualmente, e seus efeitos só terão validade após aprovação pela Diretoria da Dillon DTVM.

17.2. Esta Política é documentada e revisada, no mínimo, anualmente.

17.3. Esta Política será mantida disponível para o Banco Central do Brasil por um período de cinco anos.



Diretoria: 04 Compliance e Riscos
Área: 01 Compliance
Título: 01 CODIGO PSIC

Publicação: 05/2024
Atualização: 05/11/2025
Versão: 004

18. ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

18.1. Eu, (Nome do Colaborador), inscrito no CPF sob o nº (número do CPF), declaro ter conhecimento da Política de Segurança da Informação e Segurança Cibernética, publicada internamente, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da Dillon DTVM.

18.2. Declaro, ainda, ter ciência de que, em caso de incidente de segurança ou ameaça de incidente, devo comunicar imediatamente à área responsável por meio do e-mail especificado nesta Política.

18.3. Este documento será assinado eletronicamente.

18.4. Indicar local, dia de mês de ano.