



## 1. INTRODUÇÃO E OBJETIVO

A GDC Partners DTVM é uma distribuidora de títulos e valores mobiliários aderente aos Códigos da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA) aplicáveis às suas atividades que, por sua vez, são regulamentadas pela Comissão de Valores Mobiliários, em especial pelo estabelecido na Resolução CVM n. 17/2021.

Desse modo, em observância à (i) determinação da Resolução CMN nº 4.893/2021, (ii) ao Código de Ofertas Públicas - ANBIMA e à (iii) Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), bem como em atenção à crescente necessidade de proteção dos sistemas de informação virtual em conformidade com as boas práticas do mercado, a GDC Partners DTVM (“GDC”) elaborou e implementou a presente Política de Segurança Cibernética.

Esta Política de Segurança Cibernética (“Política”) tem como objetivo estabelecer e comunicar princípios, valores, conceitos, procedimentos, controles e diretrizes que assegurem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados nas atividades da GDC, visando a redução da ocorrência de incidentes de segurança que afetem os seus negócios.

A partir da definição de ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e digitais, esta Política objetiva viabilizar a identificação de possíveis violações de segurança cibernética; mitigando, assim, os Riscos Cibernéticos e garantindo a continuidade dos negócios em caso de incidentes.

Destaque-se que a presente Política foi elaborada considerando o porte, o perfil de risco e o modelo de negócio da GDC, em especial a natureza das operações e a complexidade de suas atividades e processos; além de observar a sensibilidade dos dados e das informações sob responsabilidade da GDC.

## 2. ABRANGÊNCIA

O disposto nesta Política se aplica a todos os funcionários, executivos, sócios, diretores, estagiários e prestadores de serviços da GDC (“colaboradores”), de modo a garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam destinados apenas ao cumprimento de suas atribuições.

É de responsabilidade de cada colaborador todo prejuízo ou dano que vier a sofrer ou causar à GDC ou a terceiros, em decorrência da não observância ao disposto nesta Política.

### 3. PRINCÍPIOS

Os ativos de informação figuram como os bens mais relevantes no mercado financeiro, uma vez que garantem a vantagem competitiva de seu detentor, sendo, portanto, imperioso trata-los com responsabilidade. Por tais motivos, a GDC sempre envidará os melhores esforços de modo a garantir a segurança dos dados sob sua custódia, assim como a qualidade e a continuidade dos serviços prestados.

Nesse sentido, as práticas implementadas serão norteadas sempre em conformidade com os princípios abaixo:

- Disponibilidade – garantir que as informações estejam acessíveis e disponíveis às pessoas previamente autorizadas;
- Integridade – garantir que as informações sejam mantidas íntegras e que não sofram modificações indevidas (acidentais ou propositais);
- Confidencialidade – garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- Acesso Controlado – garantir que o acesso às informações seja permanentemente restrito, monitorado e controlado, sendo revisto periodicamente e cancelado conforme a análise do caso concreto.

### 4. CLASSIFICAÇÃO DE DADOS E INFORMAÇÕES

Os dados e informações tratados pela GDC serão classificados consoante as categorias abaixo, tendo em vista a sua relevância:

- i. Pública – documentos cuja informação foi aprovada pela diretoria para circulação pública (interna e externa), a exemplo de relatórios anuais, material para o site e correlatos;
- ii. Interna - documentos cuja informação foi aprovada para circulação exclusivamente interna, a exemplo de memorandos internos, atas de reunião, relatórios de acompanhamento de emissões de valores mobiliários, entre outros;
- iii. Confidencial – documentos cuja informação não pode ser disponibilizada em circulação externa, pois impactaria negativamente os negócios por questões estratégicas e de gestão;
- iv. Sensível/Restrita – documentos cujas informações, internas ou confidenciais, são críticas ao desenvolvimento do negócio da GDC, de modo que (a) são acobertadas por sigilo decorrente de lei, e (b) a sua perda e/ou indisponibilidade seriam prejudiciais à realização das atividades da GDC, ao cumprimento de suas obrigações legais e à prestação adequada de seus serviços.



①

2

A GDC compartilhará as informações sensíveis sempre que instada a fazê-lo em virtude de dispositivo legal, ato de autoridade competente, requerimento de entidade reguladora e por determinação judicial.

## 5. GESTÃO E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

### 5.1. Controle de Acessos, Autenticação e Senha

Todo e qualquer acesso e uso dos sistemas de informação, bancos de dados, diretórios de rede e demais recursos será devidamente monitorado, controlado e restrito a menor permissão e privilégios possíveis.

Tais acessos e usos serão autorizados por um dos diretores, devendo ser revistos de maneira periódica e cancelados tempestivamente ao término do contrato do Colaborador ou do Prestador de Serviços, podendo, ademais, serem revogados mediante solicitação de um dos diretores ou de outro colaborador dotado de poderes para tal.

O colaborador é responsável por todos os atos executados com seu login e senha de acesso, uma vez que seu identificador é único e exclusivo, devendo seguir sempre as orientações contidas nesta Política, proibir o uso de seu equipamento por outras pessoas enquanto estiver logado e bloqueá-lo ao se ausentar.

A GDC prioriza a conscientização e disseminação da cultura de segurança cibernética entre seus colaboradores, de modo a (i) promover programas de capacitação e treinamentos periódicos direcionados aos seus colaboradores com certificação, (ii) circular memorandos internos para conscientização acerca de atualizações desta Política e de questões correlatas e (iii) prestar informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

### 5.2. Prevenção contra Vírus, Arquivos e Softwares Maliciosos

A GDC dispõe de controles de prevenção a vírus e outros softwares maliciosos providos por empresa qualificada e especializada no setor de tecnologia da informação, a qual foi contratada para realizar a manutenção preventiva e corretiva dos equipamentos (estações de trabalho e cabeamento) além de prestar suporte à rede e ao provedor de e-mails.

As dependências da GDC também contam com equipamentos (serviços de firewall) necessários à proteção da sua rede interna contra ataques hackers e para estabelecimento de barreiras protetoras entre a internet e as informações arquivadas no seu servidor e nas estações de trabalho.

### 5.3. Cópias de Segurança (*Backup*)



A execução de procedimentos de *backup* é realizada de forma periódica e pré-programada nos ativos de informação da GDC, de modo a englobar (i) um *back up* diário ao fim de cada dia útil, (ii) um *back up* semanal realizado toda sexta-feira de forma manual e em HD externo e (iii) um *back up* mensal efetuado todo último dia útil do mês; visando, assim, a mitigação do risco de perda de dados ante à ocorrência de incidentes cibernéticos.

## 6. GESTÃO DE INCIDENTES

A GDC possui controles de detecção de possíveis ataques cibernéticos em seu ambiente, tais como antivírus, *AntiSpam*, *firewall*, filtro de conteúdo, entre outros, a fim de evitar a ocorrência de incidentes. Contudo, no evento da sua ocorrência, os incidentes deverão ser imediatamente comunicados aos diretores para que sejam adotadas as medidas definidas no Plano de Ação e de Resposta a Incidentes o mais breve possível.

Os incidentes serão classificados quanto à criticidade do seu impacto na continuidade do negócio da GDC:


- i. **Muito alta ou Crítica** - incidentes que expõem dados sensíveis da companhia e de seus clientes capazes de comprometer a continuidade dos negócios;
- ii. **Alta** - incidentes que possam interromper os serviços da GDC ou de alguma maneira comprometer o adequado funcionamento de seus sistemas;
- iii. **Moderada** - incidentes caracterizados por tentativas de acesso não autorizados aos sistemas da GDC.
- iv. **Baixa** - incidentes em *hardwares* ou *softwares* que sejam solucionados através de simples manutenção ou substituição.

Após a apuração da gravidade do incidente, o respectivo Plano de Ação e de Resposta será implementado.

## 7. CONTINUIDADE DE NEGÓCIOS

O processo de gestão de continuidade de negócios tem como escopo o reestabelecimento das operações a um nível aceitável, buscando minimizar impactos e perdas de ativos da informação após um incidente de segurança cibernética por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

O supracitado processo deverá considerar, minimamente, os cenários relatados abaixo para a realização dos testes previstos na Política de Continuidade de Negócios:



- i. Verificação de possíveis vulnerabilidades que possibilitem a cópia, o acesso e/ou a extração de dados sensíveis do sistema da GDC;
- ii. Execução de testes de intrusão à base de dados;
- iii. Avaliação e estimativa do tempo de recuperação de acesso às informações de *backup* em hipótese de perda de dados sensíveis;
- iv. Estratégias para a recuperação de informações sensíveis.

## **8. PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM**

Em razão do porte e do modelo de negócio das atividades da empresa, a GDC destaca que jamais fez uso do serviço de processamento e armazenamento de dados e de computação em nuvem assim como não há previsão de critérios de decisão para a sua contratação como tampouco há previsão acerca do tema em seu Plano de Continuidade de Negócios.

## **9. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE OS INCIDENTES RELEVANTES**

A GDC compartilhará as informações acerca de seus incidentes relevantes, em especial, seus registros e análises de causa e de impacto com as demais instituições abrangidas pela Resolução CMN nº 4.893/2021. Tal compartilhamento ocorrerá por meio de iniciativas ajustadas entre as instituições, resguardados o dever de sigilo bancário, os segredos do negócio e privilegiando a livre concorrência entre os participantes do mercado.

A GDC se compromete, desde a elaboração da presente Política, a compartilhar a ocorrência de incidentes cibernéticos relevantes por meio do envio de e-mails para as demais instituições, além de disponibilizar estas informações no site da GDC.

## **10. GUARDA DE DOCUMENTOS**

Os documentos abaixo listados serão armazenados e mantidos à disposição do Banco Central do Brasil pelo período de 05 (cinco) anos consoante disposto na legislação pertinente, englobando:

- i. A Política de Segurança Cibernética em tela;
- ii. O Plano de Ação e de Resposta a Incidentes;
- iii. O Relatório Anual acerca da implementação do Plano de Ação e de Resposta a Incidentes;
- iv. Os contratos referentes à prestação de serviços relevantes de processamento, armazenamento de dados e computação;
- v. Os dados, registros e informações relativas aos mecanismos de acompanhamento e de controle da implementação e da efetividade da Política, do Plano de Ação e de Resposta a Incidentes, da Política de Continuidade dos Negócios e a documentação com os critérios que configurem uma situação de crise.



## 11. COMPROMISSO DA ALTA ADMINISTRAÇÃO

Os dispositivos apresentados nesta Política de Segurança Cibernética possuem total aderência da Alta Administração da GDC, a qual se compromete com a melhoria contínua dos procedimentos e controles aqui relacionados, com vistas a promover a sua plena e total eficácia.

## 12. VIOLAÇÃO E PENALIDADES

Atividades suspeitas, incidentes e violações de segurança deverão ser informadas aos diretores assim que a sua ocorrência for verificada, a fim de que as medidas necessárias sejam tomadas o mais breve possível.

Toda violação e/ou desvio às diretrizes desta Política será apurado para a determinação da sua extensão e posterior aplicação das sanções cabíveis aos envolvidos. O não cumprimento desta Política, intencional ou acidental, acarretará ações disciplinares e trabalhistas aos colaboradores da GDC. Já os prestadores de serviços e parceiros de negócios estão sujeitos à rescisão de seus contratos em que a GDC é parte, bem como às penas de responsabilidade civil e criminal na extensão que a lei permitir.

## 13. VIGÊNCIA

A presente Política entra em vigor em 19/11/2021 e será revisada no período máximo de 01 (um) ano ou em momento anterior ao lapso anual, conforme se faça necessário para que o documento permaneça sempre atualizado.

Esta Política foi aprovada pela Diretoria em 19/11/2021.

Rio de Janeiro, 19 de novembro de 2021.



**Juarez Dias Costa**  
Diretor Presidente



**Fritz Bernardes**  
Diretor



**Ellen Stefanie Alves Costa**

*Compliance Officer*