CARDINAL PARTNERS INVESTIMENTOS LTDA.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE SEGURANÇA CIBERNÉTICA

JUNHO 2022

Controle de versões:

| Versão | Diretor Responsável |
|---|---|
| Fev-2019 | Larissa Gomes |
| Jun-2022 | Bianca Tsutsumi |

## Sumário

# CAPÍTULO 1. INTRODUÇÃO

## 1.1 Definição e Objetivos

A Política de Segurança da Informação e de Segurança Cibernética ("Política") da CARDINAL PARTNERS INVESTIMENTOS LTDA. ("Cardinal Partners) é uma declaração formal da Cardinal Partners acerca do seu compromisso com a proteção de Informações e Segurança Cibernética (*cybersecurity*), conforme definição adiante, devendo ser cumprida por todos os Colaboradores.

Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da Informação.

Esta política visa proteger as informações, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme art. 4º, §8º, da Instrução CVM n.º 558/15, e alterações posteriores, bem como aprimorar a segurança cibernética da Cardinal Partners, nos termos do Código ANBIMA de Administração de Recursos de Terceiros, seguindo as recomendações e diretrizes do Guia de Cibersegurança da ANBIMA, editado em dezembro de 2017 e suas alterações posteriores.

Via de regra, nenhuma Informação Sigilosa deve ser divulgada, dentro ou fora da Cardinal Partners, a quem não necessite de, ou não deva ter acesso a tais informações para desempenho de suas atividades profissionais. Qualquer informação, independentemente de ser considerada Informação Sigilosa, seja sobre a Cardinal Partners, relativa às suas atividades, aos seus sócios, Fundos e Clientes dentre outras, ou obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser revelada ou fornecida ao público, à mídia, ou a terceiros de qualquer natureza da maneira e conforme previstos nos Capítulo 3, Capítulo 4 e Capítulo 5 do Manual de Compliance da Cardinal Partners, e demais documentos específicos para cada fim.

Na falta de previsão expressa, a revelação ou fornecimento somente poderá ocorrer com o conhecimento e, dependendo do caso, autorização prévia do Diretor de Gestão de Riscos e de Compliance.

## 1.2 Abrangência

A efetividade desta política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das informações e dos ativos disponibilizados pela Cardinal Partners ao Colaborador.

Esta política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de processamento da informação de propriedade ou controlados pela Cardinal Partners, sendo de responsabilidade individual e coletiva o seu cumprimento.

Todos os Colaboradores devem aderir à esta Política por escrito, conforme Anexo I. Toda alteração será comunicada e os Colaboradores confirmaram ciência e adesão às alterações via Anexo II.

1.3 Vigência

A presente Política tem vigência a partir da data de sua aprovação e comunicação e vigorará por prazo indeterminado.

1.4 Designação de um Diretor Responsável

A responsabilidade pela aplicação desta Política é da Diretora de Compliance, conforme constituído no Contrato Social da Cardinal Partners.

A Diretora de Compliance será responsável, sobretudo, pela observação da implementação dos mecanismos técnicos da Política abaixo estabelecida, bem como pela coordenação de sua revisão quando for necessário.

Não obstante, cabe a todos os Colaboradores:

- Cumprir fielmente a Política de Segurança da Informação;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela Sociedade;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Sociedade;
- Cumprir as leis e normas que regulamentam os aspectos relacionados à propriedade intelectual no que se refere às informações de propriedade ou controladas pela Sociedade e;
- Comunicar imediatamente ao Comitê qualquer descumprimento ou violação da Política de Segurança da Informação.

## CAPÍTULO 2. PRINCÍPIOS

A informação é um ativo que possui grande valor para a Cardinal Partners, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Cardinal Partners, Clientes, Fundos e Colaboradores.

As informações podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, verbalmente, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança da informação deve ser prioridade constante da Cardinal Partners, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da Cardinal Partners.

Assim, por princípio, a guarda e segurança das informações deve abranger três aspectos básicos, destacados a seguir:

- Acesso: Somente pessoas devidamente autorizadas pela Cardinal Partners devem ter acesso às informações;
- Integridade: Somente alterações, supressões e adições autorizadas pela Cardinal Partners devem ser realizadas às informações e;
- Disponibilidade: A informação deve estar disponível para os Colaboradores autorizados sempre que necessário ou for demandado.

Para assegurar os três aspectos acima, a informação deve ser adequadamente gerenciada e protegida contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em cumprimento ao Guia Anbima de Segurança Cibernética, a Cardinal Partners possui quatro pilares principais no seu programa de segurança cibernética:

- Identificação e avaliação de riscos (*risk assessment*);
- Ações de prevenção e proteção;
- Monitoramento e testes; e
- Plano de resposta.

A implantação e monitoramento da capacidade da Cardinal Partners atender a estes pilares deverá ser feito pelo Diretor de Gestão de Riscos e de Compliance. Também a fim de atingir os objetivos dispostos acima, cada segmento de atuação da Cardinal Partners terá suas próprias responsabilidades.

A Cardinal Partners deverá ter uma abordagem holística em relação à segurança cibernética, sendo obrigação do Diretor de Gestão de Riscos e de Compliance promover treinamentos para que os Colaboradores saibam as suas respectivas funções na proteção de informações sigilosas, para que possam agir de maneira apropriada frente as situações que requeiram respostas.

## CAPÍTULO 3. MODELO ADOTADO

A Cardinal Partners optou por não manter time próprio dedicado a segurança das informações, segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, inclusive para a realização de tarefas (instalações, substituições, configurações), verificações e manutenções periódicas.
Assim sendo, para implementação e monitoramento do contínuo da presente política, a Cardinal Partners conta com o suporte e assessoria de empresa terceirizada de tecnologia da informação, a INTERMÍDIA COMERCIO E SERVIÇOS LTDA., cujo nome fantasia é Intermídia Networks (https://intermidiasp.com.br/) ("Intermídia").

Dessa mesma maneira, a Cardinal Partners não mantém grupos de trabalho ou outros fóruns para tratar de segurança cibernética. Quando necessário, as matérias a esta relacionadas serão apresentadas pelo Diretor de Gestão de Riscos e de Compliance e tratadas no Comitê de Gestão de Riscos e de Compliance.

## CAPÍTULO 4. PROCEDIMENTO DE SEGURANÇA CIBERNÉTICA

### 4.1 Identificação e avaliação de Riscos (*Risk Assessment*)

A Cardinal Partners deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Código Anbima de Segurança Cibernética definiu que os ataques mais comuns de criminosos cibernéticos (*cybercriminals*) são os seguintes:

- Malware (vírus, cavalo de troia, spyware e ransomware);
- Engenharia Social;
- Pharming;
- Phishing scam;
- Vishing;
- Smishing;

- Acesso pessoal;
- Ataques de DDoS e botnets; e
- Invasões (advanced persistent threats).

## 4.2 Ações de Prevenção e Proteção

A Cardinal Partners adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores. A Cardinal Partners trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.
Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a Cardinal Partners deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A Cardinal Partners conta com recursos anti-malware em todas as estações.

Os servidores locais físicos, mais vulneráveis à todo tipo de ataque, foram extintos e atualmente a Cardinal Partners utiliza os servidores em ambiente de nuvem da Microsoft.

A utilização do Microsoft Azure garante à Cardinal Partners a conformidade com as normas internacionais de segurança e privacidade, bem como processos rigorosos de auditoria aos quais a Microsoft é submetida regulamente, podendo oferecer um produto seguro e com baixo risco à segurança da informação.

O recurso em nuvem possibilita o backup das informações de forma segura, contínua e automatizada, com a possibilidade de rastreamento no caso de uso indevido ou vazamento de informação.

## 4.3 Monitoramentos e testes

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na Cardinal Partners ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito à monitoramento em tempo real, inclusive em equipamentos pessoais acessados durante o expediente da Cardinal Partners. Esse monitoramento é realizado

automaticamente (software e/ou hardware), pela Área de Gestão de Riscos e de Compliance e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da Cardinal Partners, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A Cardinal Partners possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de hardware e software atualizados, bem como os sistemas operacionais e softwares de uso atualizados.
Periodicamente, a Cardinal Partners realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, em linha, inclusive, com o Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Cardinal Partners. Dentre as medidas, incluem-se, mas sem se limitar:

- Verificação dos logs dos Colaboradores;
- Alteração periódica de senha de acesso dos Colaboradores;
- Segregação de acessos;
- Manutenção trimestral de todo os hardwares; e
- Backup diário, realizado na nuvem.

Sem prejuízo dos testes realizados pela Intermídia, a Cardinal Partners acompanha os testes, o desenvolvimento e as atualizações disponíveis tanto pelo provedor atual, como pelos correntes de mercado, mantendo-se em linha com a velocidade com que o mercado de cibersegurança evolui.

### 4.4 Plano de resposta

Havendo indícios ou de suspeita fundamentada, a Intermídia deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

Na hipótese de vazamento de Informações Sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Manual de Compliance e Código de Conduta Ética.

Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão ser formalizados em relatório para deliberação durante o Comitê de Gestão de Riscos e de Compliance. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação do comitê deverão, ser registrados por escrito e divulgado a todos os sócios e responsáveis pelas áreas.

## CAPÍTULO 5. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

### 5.1 Adoção de comportamento seguro

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção e salvaguarda das informações que os Colaboradores adotem comportamento seguro e consistente com o objetivo de proteção das informações da Sociedade, com destaque para os seguintes itens:

- Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção da informação;
- Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das informações da Cardinal Partners, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação em uso e aos servidores;

- Todo tipo de acesso à informação da Sociedade que não for explicitamente autorizado é proibido;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- A senha do Colaborador é pessoal e intransferível, não podendo ser compartilhada, divulgada a terceiros (inclusive outros Colaboradores), anotada em papel ou em sistema visível ou de acesso não-protegido;
- Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;
- Somente *softwares* homologados pela Sociedade podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de serviços de informática da Sociedade;
- Arquivos eletrônicos de origem desconhecida nunca devem ser abertos e/ou executados;
- Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter informações confidenciais e/ou legalmente privilegiadas. Não podem ser parciais ou totalmente reproduzidos sem o consentimento do autor. Qualquer divulgação ou uso não autorizado de mensagens eletrônicas e/ou seus anexos é proibida;
- Documentos impressos e arquivos contendo informações sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da Cardinal Partners sem a autorização prévia do superior hierárquico do Colaborador;
- O acesso remoto à rede, às Informações Sigilosas e sistemas da Cardinal Partners somente será permitida mediante autorização do Diretor de Gestão de Riscos e de Compliance e desde que seja estritamente necessário para o desempenho das funções do Colaborador. O Colaborador será corresponsável pela segurança do acesso remoto aos sistemas e informações da Sociedade;
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação deve ser imediatamente esclarecido com o superior hierárquico imediato, o qual levará a dúvida ao Comitê, se for necessário.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Cardinal Partners. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos

que possam causar constrangimento à terceiros, bem como com conteúdo político ou outro que possa colocar a Cardinal Partners em risco.

5.2 Gestão de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos

Todo acesso às informações e aos ambientes lógicos da Sociedade deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação ou responsável por sua guarda e preservação.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

- Pedido formal de concessão e cancelamento de autorização de acesso ao usuário aos sistemas de informação;
- Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações;
- Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de Segregação das Atividades (descrita no Capítulo 3 do Manual de Compliance);
- Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da Sociedade, ou que tenham mudado de função, se for o caso e;
- Revisão periódica das autorizações concedidas.

5.3 Controle de Comunicações e Mensagens Eletrônicas

A Cardinal Partners considera que todos os dados mantidos e circulados através dos canais de comunicações eletrônicas, sejam estes transmitidos, recebidos ou contidas nos equipamentos eletrônicos de comunicação da empresa são de propriedade desta.

Os sistemas, informações e serviços utilizados pelos Colaboradores são de exclusiva propriedade da Sociedade, não podendo ser interpretados como de uso pessoal.

Todos os Colaboradores devem ter ciência de que o uso das informações e dos sistemas de informação da Sociedade é monitorado, e que os registros assim obtidos poderão ser utilizados

para detecção de violações das políticas da Cardinal Partners e conforme o caso, servir como evidência em processos administrativos e/ou legais.

E-mail, telefones e quaisquer outras modalidades de sistema de comunicação devem ser utilizados somente para os negócios da CARDINAL PARTNERS. Informações de cunho pessoal, divulgadas através desses sistemas não serão consideradas como confidenciais.

Para assegurar o fiel cumprimento de suas regras internas, a CARDINAL PARTNERS se reserva no direito de rastrear, monitorar, gravar e inspecionar o tráfego de internet, intranet, sistema de mensagem instantânea, correio físico e eletrônico, bem como arquivos armazenados pertencentes à empresa ou utilizados em nome dela.

Para fins de monitoramento e rastreabilidade destes canais de comunicação serão utilizados mecanismos automáticos de filtro de dados que disporá de gatilhos, que serão acionados quando do uso de determinadas expressões ou palavras chaves, sejam na forma escrita ou expressadas nas trocas de e-mails ou em correspondências impressas.
Os monitoramentos eletrônicos serão procedidos periodicamente e intempestivamente sempre que solicitado pelo Comitê de Compliance, em dias e horas aleatórias, por amostragem, via verificações manuais ou eletrônicas, nas contas de e-mails corporativos dos colaboradores.

Desta forma, estão sujeitos às regulamentações e políticas internas de fiscalização da empresa. Os colaboradores não devem esperar privacidade ao se utilizar de tais meios de comunicação.

## CAPÍTULO 6. DISPOSIÇÕES GERAIS

Em cumprimento ao art. 14, III, da Instrução CVM nº 558/15, a presente política está disponível no endereço eletrônico da Cardinal Partners: http://www.cardinalpartners.com.br/

**********

## ANEXO I

## TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito(a) no CPF/MF sob o nº _____, na qualidade de Colaborador da Sociedade, pelo presente instrumento, atesto que:

I – Recebi uma cópia da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA da CARDINAL PARTNERS INVESTIMENTOS LTDA ("Política" e "Cardinal Partners");

II - Tomei ciência dos direitos e obrigações a que estou sujeito, inclusive no que se refere ao bom uso das informações e dos ativos disponibilizados pela Cardinal Partners;

III – Estou ciente de que o uso das informações e dos sistemas de informação da CARDINAL PARTNERS é monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações à Política e, conforme o caso, servir como evidência em processos administrativos e/ou legais;

IV – Estou de acordo com o inteiro teor da Política e, especialmente, aos princípios de acesso, integridade e disponibilidade;

Declaro ter lido e aceito integralmente os termos e regras do Manual, expressando total concordância e irrestrita adesão aos referidos termos e regras, sobre os quais declaro não ter dúvida.

São Paulo, [Data]

_____

**[nome completo]**

## ANEXO II

## TERMO DE ADESÃO ÀS ALTERAÇÕES À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito(a) no CPF/MF sob o nº _____, na qualidade de Colaborador da Sociedade, pelo presente instrumento, atesto que:

I – Recebi uma cópia da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA da CARDINAL PARTNERS INVESTIMENTOS LTDA ("Política" e "Cardinal Partners");

II – Estou ciente sobre as alterações promovidas na Política;

III – Estou ciente de que o uso das informações e sistemas de informação da Sociedade é monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações ao Manual e, conforme o caso, servir como evidência em processos administrativos e/ou legais; e

IV – Estou de acordo com o inteiro teor da Política e, especialmente aos princípios de acesso, integridade e disponibilidade;

Declaro ter lido e aceito integralmente os termos e regras da Política, expressando total concordância e irrestrita adesão aos referidos termos e regras, sobre os quais declaro não ter dúvida.

São Paulo, [Data]

_____

**[nome completo]**