PATAGÔNIA

CAPITAL

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

AGOSTO 2023

PATAGÔNIA
CAPITAL

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. Introdução

A presente Política de Segurança Cibernética e da Informação ("Política") da Patagônia Capital Gestora de Recursos Ltda. ("Gestora") formaliza e esclarece regras, procedimentos e controles internos para fins de proteção de dados e de segurança cibernética e da informação.

Em atenção aos dispositivos da Resolução CVM nº 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, à Lei 13.709, de agosto de 2018 ("Lei Geral de Proteção de Dados"), e em observância ao Guia de Cibersegurança ANBIMA, a Gestora procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

2. Objetivo

Esta Política tem o objetivo de estabelecer as diretrizes, princípios, responsabilidades e orientações relacionadas ao tratamento das informações ao uso adequado de ativos e recursos tecnológicos pelos Colaboradores da Gestora e Terceiros e à proteção de tais ativos e recursos tecnológicos, contribuindo para o aprimoramento da segurança, tanto informacional quanto cibernética da Gestora, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

3. Abrangência

Esta Política é aplicável aos sócios, integrantes de cargos de administração ou gestão, funcionários, estagiários e demais Colaboradores, independentemente do vínculo contratual ou societário que mantenham com a Gestora ("Colaboradores"), bem como a todos os terceiros, partes interessadas nos negócios da Gestora, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestora, ou que acessem informações a ela pertencentes ("Terceiros").

Nesse sentido, todos os Colaboradores da Gestora devem conhecer e obedecer aos termos desta Política.

4. Segurança Cibernética e da Informação

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

A Política de Segurança Cibernética e da Informação leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora.

O Diretor de Compliance é a pessoa responsável na Gestora para coordenar diretamente as atividades e tratar sobre as questões relacionadas à presente Política. Caso seja verificada necessidade, serão contratados terceiros especializados nesta área para, juntamente com o Diretor de Compliance, analisar no caso concreto a vulnerabilidade, ameaças e impactos sobre os ativos de informação da Gestora, sendo realizadas as recomendações de proteções adequadas.

5. Princípios básicos

Os seguintes princípios básicos norteiam esta política:

(i) Confidencialidade;

(ii) Treinamento e conscientização sobre segurança cibernética e da informação para todos os Colaboradores;

(iii) Testes periódicos dos sistemas.

6. Identificação de Riscos (Risk Assessment)

A Gestora, no âmbito de suas atividades, identificou os seguintes principais riscos internos e externos que precisam de proteção:

(i) **Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo, correspondências eletrônicas e físicas);

(ii) **Sistemas:** informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros;

(iii) **Processos e Controles:** processos e controles internos que sejam parte da rotina das áreas de negócio e compliance da Gestora; e

(iv) **Governança da Gestão de Risco:** a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Além disso, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, em linha com o disposto no Guia de Cibersegurança da ANBIMA:

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

(v) **Malware:** softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);

(vi) **Engenharia social:** métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

(vii) **Ataques de DDoS (*distributed denial of services*) e botnets:** ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

(viii) **Invasões (advanced persistent threats):** ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Diante do que foi apresentado, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

7. Procedimentos e Condutas de Prevenção e Proteção

Regras Gerais

(i) Os arquivos físicos com os dados e informações relativos à atividade de administração de carteira de valores mobiliários e gestão de fundos de investimento desenvolvidos pela Gestora ficarão alocados, quando físicos, na sede social da Gestora e quando digitais, no *SharePoint* Corporativo da Gestora, sendo que apenas os Colaboradores cujas atividades forem relacionadas com a gestão, terão acesso às informações confidenciais e sigilosas relativas à sua atividade.

(ii) Os equipamentos e computadores disponibilizados aos Colaboradores da Gestora deverão ser utilizados com a finalidade de atender aos interesses comerciais da Gestora, sendo permitida a sua utilização para fins particulares de forma moderada e que, de nenhuma forma, possa trazer riscos aos sistemas utilizados pela Gestora para realização de seus fins comerciais.

(iii) A gravação de cópias de arquivos e instalação de programas em computadores da Gestora deverá respeitar as regras estabelecidas no presente Código de Conduta.

(iv) Downloads podem ser realizados desde que sejam relacionados à atividade comercial da Gestora e/ou de aplicativos e sistemas amplamente conhecidos pelo mercado e de uso diário de cada usuário. Periodicamente, a critério do Diretor de

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

Compliance, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

(v) O correio eletrônico disponibilizado pela Gestora ("**E-mails Corporativos**") caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização preferencial voltada para alcançar os fins comerciais aos quais se destina.

(vi) As mensagens enviadas ou recebidas por meio de E-mails Corporativos, seus respectivos anexos e a navegação por meio da rede mundial de computadores por meio de equipamentos da Gestora ou dentro das instalações da Gestora poderão ser monitoradas.

(vii) Os E-mails Corporativos recebidos pelos Colaboradores da Gestora, quando abertos, deverão ter seu conteúdo verificado pelo Colaborador, não sendo admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem. Os arquivos de E-mails Corporativos poderão ser inspecionados pela Gestora, a critério do Diretor de Compliance, a qualquer tempo e independentemente de prévia notificação.

(viii) Cada um dos Colaboradores da Gestora, no momento de sua contratação, receberá uma senha secreta, pessoal e intransferível para acesso aos computadores, à rede corporativa e aos E-mails Corporativos da Gestora, que será imediatamente desativada no caso de desligamento do respectivo Colaborador.

(ix) O acesso a informações confidenciais e sigilosas será restrito e diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Gestora a critério do Diretor de Compliance. O controle de acesso a tais informações será realizado por meio da liberação ou não, pelo Diretor de Compliance, às pastas do *Share Point* da Gestora que possuem tais informações.

(x) Cada Colaborador terá acesso a pastas eletrônicas diretamente relacionadas às atividades desenvolvidas pela sua área. Apenas o prestador de serviços de tecnologia e o Diretor de Compliance da Gestora terão acesso a todas as pastas.

(xi) As combinações de login e senha do SharePoint / e-mail Corporativo são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte restrita da rede da Gestora necessária ao exercício de suas atividades. Assim, cada login está vinculado a uma senha única, de forma que todas as atividades realizadas por tal Colaborador ficarão registradas e poderão ser monitoradas para fins de averiguar quaisquer condutas suspeitas.

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

(xii) Todas as instalações da Gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade de todas e quaisquer informações.

(xiii) O acesso de terceiros à sede da Gestora somente é permitido na recepção e nas salas de reunião. O acesso físico a áreas em que informações confidenciais ou proprietárias possam estar presentes ou ser discutidas é limitado e restrito aos Colaboradores da respectiva área. As reuniões com terceiros não poderão ser conduzidas nas salas dos Colaboradores e quaisquer trabalhos em projetos confidenciais deverão ocorrer em áreas fisicamente separadas e seguras.

(xiv) As estações de trabalho são fixas, com computadores seguros e as sessões abertas devem ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

(xv) É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à mesma com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais e, em respeito à Lei de Propriedade Intelectual, pertencem à Gestora.

(xvi) A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

(xvii) Todo Colaborador que tiver acesso aos sistemas de informação da Gestora é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não os divulgar a terceiros em qualquer hipótese.

(xviii) O ativo de maior valor da Gestora são as Informações Confidenciais e privilegiadas da própria Gestora, dos seus clientes e eventualmente de outras companhias com as quais a Gestora, seus clientes ou sócios tenham vínculo, por isso, os sistemas de segurança visam preservar o sigilo dessas informações.

(xix) Em complementação aos procedimentos acima, que deverão ser observados por todos os Colaboradores, a Gestora possui firewall de segurança devidamente contratado e instalado nos servidores para acesso à sua rede, visando manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O pacote de segurança cibernética da Gestora é o *GravityZone Business Security*, da Bitdefender, que garante proteção completa contra todos os tipos de malware (ransomware,

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

phishing, ataque de dia zero, vírus, spyware etc.), e será atualizado diariamente. Adicionalmente, o backup de arquivos é realizado diariamente tanto online, pelo Share Point da Gestora, quanto offline, por meio de servidor físico *Time Machine* da Apple, com o *Capsule HD - AirPort Time Capsule de 1,2T*. Com relação ao acesso à internet, possuímos duas redes (Vivo e MD Net), distintas possibilitando alternativa em caso de queda de uma delas, bem como segregação de acesso entre clientes/Terceiros e nossos Colaboradores.

(xx) Novas tecnologias de solução de backup, serão estudadas para futuras implementações, conforme necessidade da Gestora e orientação do Diretor de Compliance, ouvido os técnicos de informática e o setor responsável. Através de software de monitoramento remoto seguro, o prestador de serviços de tecnologia poderá otimizar o controle sobre a rede.

(xxi) A Gestora oferece treinamentos periódicos aos quais os Colaboradores são submetidos durante o ano, com o objetivo de conscientizá-los sobre confidencialidade das informações, cibersegurança, engenharia social, phishing, entre outras potenciais ameaças à integridade dos sistemas de informação.

(xxii) Periodicamente serão realizados testes de segurança no sistema de informação da Gestora, incluindo as seguintes práticas: (a) alteração das senhas de acesso dos Colaboradores; (b) testes no firewall; (c) manutenção dos aparelhos eletrônicos; (d) testes nos sistemas de backup; (e) testes nas eventuais restrições impostas aos diretórios; e (f) testes de invasão externa e phishing.

(xxiii) Anualmente ou sempre que entender necessário, o Diretor de Compliance irá avaliar e revisar os procedimentos adotados pela Gestora para garantia da segurança cibernética e das informações. Além disso, sempre que possível, serão tomadas medidas para atualização da avaliação dos riscos aos quais a Gestora esteja exposta.

Dessa forma, de modo a proteger o vazamento de Informações Confidenciais de propriedade da Gestora, são adotados os mecanismos mencionados na presente Política de Segurança Cibernética e da Informação, quais sejam, realização de backup regularmente, testes de segurança periódicos, treinamentos periódicos aos Colaboradores, controle de acesso às informações, proteção física e manutenção dos aparelhos eletrônicos, instalação de firewall de segurança e atualização dos antivírus.

8. Plano de Identificação e Resposta

Caso, mesmo após as ações de prevenção e proteção, seja verificado o vazamento de informações da Gestora ou dos seus clientes, independentemente de descumprimento da presente Política, a Gestora tomará todas as medidas cabíveis e com a menor brevidade possível para amenizar as consequências do vazamento das referidas informações.

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

Identificação de Suspeitas

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais ou dados pessoais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance prontamente. O Diretor de Compliance determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação. No caso de o vazamento de informações envolver dados pessoais, caso necessário, o Diretor de Compliance notificará, em prazo compatível com a severidade do evento, a Autoridade Nacional de Proteção de Dados.

Procedimento de Resposta

O Diretor de Compliance responderá a qualquer informação de suspeita de violação, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora de acordo com os critérios abaixo:

(i) Avaliação de tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, administrador fiduciário, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, a fim de garantir ampla disseminação e tratamento equânime da informação, se privilegiada); e

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

(vii) Determinação do responsável que arcará com as perdas decorrentes do incidente, a cargo do Comitê de Compliance, após condução de investigação e uma avaliação completa das circunstâncias do incidente.

(viii) Se verificado que qualquer Colaborador infringiu as normas aqui estipuladas, principalmente em relação à Política de Segurança Cibernética e da Informação, referido Colaborador poderá ser responsabilizado pelas perdas e danos incorridos em razão da sua conduta irregular, além das demais sanções a serem aplicadas pelo Diretor de Compliance.

9. Proteção de Dados Pessoais

Escopo e Abrangência

A Gestora está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Gestora, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Gestora.

É importante observar que o escopo da proteção de dados pessoais no âmbito da Gestora está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas e comerciais. Também estão abrangidos por esta proteção os dados de candidatos às vagas na Gestora, de fornecedores e outros com os quais a Gestora manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Gestora está pautado nos requisitos do artigo 7º da Lei Geral de Proteção de Dados, assim como nas premissas do artigo 11 da mesma Lei, quando aplicável. Dessa maneira, o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

(i) quando o titular consentir, de forma específica e clara, para finalidades específicas;

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

(ii) sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

(iii) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

(iv) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

(v) proteção da vida ou da incolumidade física do titular ou de terceiro;

(vi) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

(vii) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei Geral de Proteção de Dados e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Princípios Norteadores

A Gestora também se compromete a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios elencados no art. 6º da Lei Geral de Proteção de Dados.

Direitos

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18, da Lei 13.709/2018, o titular dos dados pessoais tem direito realizar solicitações à Gestora com relação aos seus dados, a qualquer momento e mediante requerimento expresso. O exercício de tais direitos em face da Gestora deve ser analisado em cada caso concreto.

A Gestora disponibiliza canal de comunicação, através do endereço dados@patagoniacapital.com.br, por meio do qual o seu Diretor de Compliance receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na Lei Geral de Proteção de Dados.

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

Período de Armazenamento dos Dados Pessoais

Os dados pessoais serão armazenados pela Gestora durante o período necessário para o atingimento dos objetivos para os quais foram coletados. Porém, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual.

Transferência Internacional de Dados Pessoais

Em certas situações a Gestora poderá realizar a transferência internacional de dados pessoais a partir do envio de informações e documentos, a fim de possibilitar procedimentos junto à prestadores de serviços internacionais. Esta transferência é realizada segundo os parâmetros do artigo 33, II da Lei Geral de Proteção de Dados.

Cooperação com Autoridades

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Gestora estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à Gestora, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Gestora cooperará com a Autoridade Nacional de Proteção de Dados (ANPD) em qualquer problema em relação à proteção de dados e dentro dos limites previstos na Lei e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Governança

As matérias relacionadas aos dados pessoais, dados sigilosos e seus tratamentos serão apresentados pelo Diretor de Compliance para deliberação no Comitê de Compliance e Risco.

10. Revisão desta Política

A área de Compliance da Gestora, coordenada pelo Diretor de Compliance, deverá realizar uma revisão da Política de Segurança da Informação e Cibernética a cada 12 (doze) meses, no mínimo, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, incluindo no relatório anual de compliance eventuais deficiências encontradas.

(16) **3620-2333**
www.patagoniacapital.com.br
Av. Braz Olaia Acosta, 727 – Sala 1101
Jardim Califórnia, Ribeirão Preto - SP, 14026-040

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Gestora e acontecimentos regulatórios relevantes

O Diretor de Compliance visará promover a aplicação da presente Política de Segurança Cibernética e da Informação, bem como o controle, a supervisão e a aprovação de exceções, sendo sua responsabilidade assegurar a implementação de mecanismos eficientes capazes de resguardar a segurança das informações de propriedade da Gestora ou de terceiros em relação às quais a Gestora tenha tido acesso, bem como a identificação de quaisquer infrações às regras aprovadas nesta Política.