**MOAT CAPITAL GESTÃO DE RECURSOS LTDA.**

# Política de Segurança da Informação e Segurança Cibernética

**Versão Atualizada**
**Novembro de 2021**

## ÍNDICE

## I. OBJETIVO E ABRANGÊNCIA

O objetivo desta Política de Segurança da Informação e Segurança Cibernética ("Política") da Moat Capital Gestão de Recursos Ltda. ("Moat Capital") é garantir a proteção, a manutenção de privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que disciplinam, em nível estratégico, os princípios fundamentais incorporados pela Moat Capital para o alcance dos objetivos de segurança da informação, bem como um programa de segurança cibernética contra ameaças, nos termos da Instrução da Comissão de Valores Mobiliários nº 558, de 26 de março de 2015, conforme alterada ("ICVM 558"), do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, vigente desde 1 de julho de 2021 ("Código de Recursos de Terceiros ANBIMA") e do Guia de Cibersegurança da ANBIMA, de 06 de dezembro de 2017 ("Guia de Cibersegurança").

Essa Política demonstra o compromisso em zelar e tratar todas as informações de propriedade e/ou sob guarda da Moat Capital, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Demonstra também o compromisso com os aspectos regulatórios e estratégicos da Moat Capital, estando assim, em conformidade com as principais regulamentações vigentes.

## II. APLICABILIDADE

As regras enunciadas nesta Política se aplicam a todos os Colaboradores, prestadores de serviço, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Moat Capital, ou que acesse informações a ela pertencentes, ainda, todo e qualquer usuário de recursos computadorizados da Moat Capital tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

## III. REGRAS GERAIS

A Moat Capital considera que os ativos de informações são os bens mais importantes no mercado financeiro, portanto, tratá-los com responsabilidade e segurança são os principais compromissos. Dessa forma, um dos principais objetivos é contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Moat Capital, visando a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes

oriundos de ataques cibernéticos ou que possam causar prejuízo para as atividades desenvolvidas internamente.

As informações geradas e recebidas devem abranger:

(i) Disponibilidade: visa garantir que todas as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
(ii) Integridade: visa garantir que a informação esteja sempre completa e íntegra e que não tenha sido modificada ou destruída de maneira indevida (não autorizada ou acidental) durante o seu ciclo de vida;
(iii) Confidencialidade: visa garantir a verificação da identidade dos usuários e a certeza de que a informação provém da origem anunciada;
(iv) Auditoria: visa assegurar o cumprimento da política geral de segurança da informação; e
(v) Riscos Cibernéticos: riscos de ataques cibernéticos, oriundos de *softwares* maliciosos (*malware*), técnicas de engenharia social, invasões, ataques de rede (DDoS, Botnets, etc.), fraudes externas, exposição de dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

No mais, a Moat Capital 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, em consonância com o disposto na ICVM 558, no Código de Recursos de Terceiros ANBIMA e no Guia de Cibersegurança.

A identificação de possíveis ataques é feita através de controles de detecção implementados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamento malicioso, antivírus, antispam, entre outros, como veremos adiante nesta Política.

Importante ressaltar que os Colaboradores e terceiros da Moat Capital são treinados, periodicamente, sobre os conceitos de segurança da informação, através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética.

## IV. INFORMAÇÕES CONFIDENCIAIS

O acesso as Informações Confidenciais, incluindo dados pessoais, coletados e armazenados pela Moat Capital é restrito as pessoas autorizadas, e necessário à prestação de seus serviços, sendo vedado o uso para quaisquer outras finalidades, devendo respeitar, ainda, o disposto no ISO 27001 (Segurança da Informação).

A Moat Capital, apenas poderá divulgar as Informações Confidenciais nas seguintes hipóteses:

(i) Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
(ii) Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela Moat Capital a defender seus direitos e créditos;
(iii) Aos órgãos reguladores do mercado financeiro; e
(iv) Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

As medidas acima expostas têm como intuito mitigar a possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação as Informações Confidenciais.

## V. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA

O gerenciamento dos controles de segurança visa assegurar que os procedimentos operacionais sejam desenvolvidos, implementados, mantidos ou modificados de acordo com os objetivos estabelecidos nesta Política. Para implementação e monitoramento contínuo a Moat Capital conta com o suporte e assessoria da empresa terceirizada de tecnologia da informação Tecnoqualify Consultoria e Comércio Ltda ("Tecnoqualify").

**Identificação de Risco:** Os riscos podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. Sendo que os métodos mais comuns de ataques cibernéticos são os seguintes:

**a)** *Software* Malicioso (*Malware*): São *softwares* desenvolvidos para corromper computadores e redes. Sendo assim, todos os ativos que estejam conectados à rede corporativa ou façam uso de informações da Moat Capital, devem, sempre que compatível, serem protegidos com uma solução *anti-malware* determinada pela área de Segurança da Informação.
Os *malwares* mais comuns são: (i) vírus; (ii) cavalo de tróia; (iii) *spyware*; e (iv) *ransomware*.

**b)** Engenharia Social: São métodos de manipulação para obter Informações Confidenciais, como senhas, dados pessoais, dados bancários, número de cartão de crédito, entre outras. Sendo que as formas mais comuns são:
Pharming: direciona o Colaborador para um site fraudulento, sem o seu conhecimento;

Phising: através de um link transmitido por e-mail, simulando ser uma pessoa ou empresa confiável, envia uma comunicação eletrônica oficial para obter Informações Confidenciais;
Vishing: através de ligação telefônica, simulando ser uma pessoa ou empresa confiável para obter Informações Confidenciais;
Smishing: através de mensagem de texto, simulando ser uma pessoa ou empresa confiável para obter Informações Confidenciais; e
Acesso Pessoal: pessoas em lugares públicos como bares, cafés e restaurantes, captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque cibernético.

**c)** Ataques de DDoS (*Distributed Denial of Services*) e Botnets: São ataques cibernéticos que tem como propósito negar ou atrasar o acesso aos serviços ou sistemas da instituição. Os Botnets, por exemplo, são ataques feitos através de um grande número de computadores infectados, utilizados para criar e mandar vírus, spam ou carregar uma rede com mensagens resultando na negação de serviços.

**d)** Invasões (*Advanced Persistent Threats*): São ataques cibernéticos realizados por invasores considerados sofisticados, ou seja, são invasores que utilizam técnicas, conhecimento e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Além dos riscos de ataques cibernéticos dispostos acima, a Moat Capital também pode estar sujeita a má funcionalidade dos sistemas internos utilizados, bem como atos/omissões de seus Colaboradores, que podem acarretar na perda e/ou na adulteração de dados e Informações Confidenciais.

**Ações de Prevenção e Proteção:** Como forma de prevenir e proteger a Moat Capital de eventuais ataques cibernéticos que podem acarretar vazamento de dados e Informações Confidenciais, ou ainda, perda, é necessário fazer um controle, através de definição do grau de sensibilidade das informações, assim como aquelas que teriam maior impacto financeiro, operacional e reputacional, em caso da ocorrência de uma das hipóteses acima elencadas.

O grau de sensibilidade das informações pode ser classificado em:

**a)** Nível I: Informações e/ou dados que a Moat Capital (a.i) tiver acesso ou conhecimento por se tratarem de informações de domínio público; (a.ii) não estiver sujeita ao compromisso ou acordo de confidencialidade; ou (a.iii) que tiver a obrigatoriedade de divulgação por lei ou autoridade competente.

**b)** Nível II: Informações e/ou dados que venham a ter a divulgação obrigatória por lei ou por autoridade competente e, no entanto, ainda não ocorreram.

**c)** Nível III: Informações e/ou dados confidenciais, tais como: técnicas, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Moat Capital, operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Moat Capital ou, ainda, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Moat Capital e/ou de seus sócios e clientes.

De acordo com o grau de sensibilidade definido acima, a Moat Capital irá segregar as informações e/ou dados e a partir disso desenvolver e manter controles, para aperfeiçoar o processo de manuseio, armazenamento, transporte e descarte de informações e/ou dados.

**Estrututa de Tecnologia da Informação e Propriedade dos Recursos:** Como forma de prevenir e proteger as informações e/ou dados, a Moat Capital estruturou a Área de Tecnologia da Informação, além da contratação da Tecnoqualify, para estabelecer os principais equipamentos, procedimentos e sistemas a serem utilizados.

A estrutura de tecnologia da Moat Capital conta com os seguintes recursos: (i) *desktops*; (ii) servidor nuvem; (iii) sistema de *Nobreak*; (iv) gerador de energia com autonomia de; (v) provedor de internet; (vi) *firewall* e proteção *fortigate*; (vii) *backup*, o processo de execução de *backup* é realizado, periodicamente, nos ativos de informação da Moat Capital, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes; e (viii) antivírus.

Além da estrutura acima apresentada, os acessos dos Colaboradores são segregados. Dessa forma, cada área interna tem uma estrutura de armazenamento de informações segregada das demais, assim como acesso limitado as outras estruturas, garantindo assim que apenas os Colaboradores autorizados e necessários para o desempenho de determinada atividade tenham acesso aquela informação.

As Áreas de Tecnologia da Informação e Compliance, são responsáveis por definir a estrutura de segregação do armazenamento e acesso de informações e/ou dados, assim como instalação de programas fora da lista autorizada e avaliação de liberações pontuais para armazenamentos e

acessos. Os acessos são revistos periodicamente, para verificar as concessões e cancelados tempestivamente ao encerramento das atividades dos Colaboradores ou prestador de serviço.

Todos os recursos de computadores e sistemas utilizados e disponibilizados para os Colaboradores são de propriedade da Moat Capital, não sendo permitida a utilização de notebooks, tablets ou outros hardwares pessoais para desempenho das atividades, salvo mediante expressa permissão da Área de Compliance. É vedada a utilização dos computadores disponibilizados para quaisquer outros fins que não sejam as atividades profissionais desempenhadas na Moat Capital.

Por último, os equipamentos e instalações de processamento de informações (crítica ou sensível) são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

**Disponibilização e Uso:** Todos os computadores disponibilizados para os Colaboradores da Moat Capital, devem ser utilizados exclusivamente para as atividades profissionais, não devendo ser utilizados para quaisquer outras finalidades.

A disponibilização e uso dos computadores devem respeitar as seguintes diretrizes: (i) cada Colaborador terá um usuário próprio, bem como acesso as estruturas cibernéticas necessárias para o desempenho das suas atividades; (ii) todos os equipamentos serão preparados e instalados pela Tecnoqualify com a supervisão da Área de Tecnologia da Informação, assim como possíveis substituições e reparos; (iii) a identificação do usuário é feita através de login e senha, a senha será alterada a cada 3 (três) meses; e (iv) todos os eventos de login e alteração de senhas são auditáveis e rastreáveis.

**Softwares:** Todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são instalados, implementados e configurados pela Tecnoqualify, mediante supervisão da Área de Tecnologia da Informação.

O Colaborador não tem permissão para instalar novos programas, alterar as configurações ou implantar ou alterar componentes físicos em seus computadores em seu usuário. É permitida a conexão de telefones celulares diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso, já a conexão de computadores pessoais é permitida desde que solicitada a Área de Compliance.

**Registros:** A Moat Capital mantém logs de sistemas, além de verificar regularmente quaisquer desvios de padrão de todos os computadores, arquivos em rede, softwares, hardwares ou acessos que não sejam autorizados, como forma de proteger contra adulterações. Os registros mantidos permitem a realização de auditorias e inspeções, conforme determina o artigo 4º, § 8º da ICVM 558.

Responsabilidades dos Usuários: O Colaborador é responsável pelos recursos disponibilizados à ele, devendo garantir a integridade física dos equipamentos e seu perfeito funcionamento.

Em relação ao comportamento, o Colaborador não deve: (i) não deve compartilhar e nem divulgar sua senha à terceiros; (ii) transportar Informações Confidenciais, sem a devida autorização e proteção; (iii) discutir assuntos confidenciais em ambientes públicos; (iv) abrir nenhuma mensagem ou e-mail de origem desconhecida ou links suspeitos, mesmo que advindos de origem conhecida; (v) deixar de armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contenham Informações Confidenciais; (vi) deixar de seguir corretamente as diretrizes para o uso de Internet e correio eletrônico estabelecidas nesta Política; (vii) sempre que se ausentar da sua estação de trabalho deve acionar a proteção de tela no computador e/ou proteção de ausência.

**Regras e Responsabilidades do Uso da Internet:** O Colaborador é responsável por todo acesso realizado com as suas credenciais e quando se comunicar através da Moat Capital deve sempre agir de modo a resguardar a imagem da Moat Capital, evitando ainda websites de fontes não seguras ou não conhecidas, salvo se autorizado pelas Áreas de Compliance e de Tecnologia da Informação.

É proibido pelo Colaborador acessar websites que possam: (i) violar direitos de autor, marcas, licenças de softwares ou patentes existentes; (ii) conter qualquer conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia; (iii) defender atividades ilegais, menosprezar, depreciar ou incitar o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física; e (iv) ter origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

**Bloqueio de Endereços de Internet:** Os acessos a websites são revisados periodicamente como forma de bloquear qualquer página que não esteja alinhada com as diretrizes impostas nesta Política.

**Uso de Correio Eletrônico:** É proibido aos Colaboradores utilizar o correio eletrônico pessoal, salvo em casos de contingência com a devida autorização da Área de Compliance.

A Moat Capital disponibiliza endereço de seu correio eletrônico para cada um dos Colaboradores desempenharem suas atividades, sendo este: individual, intransferível e não deve ser utilizado sob nenhuma hipótese para fins particulares.

É permitida a existência de endereços de correio eletrônico para envio de comunicação interna da Moat Capital.

**Acesso à Distância ao Correio Eletrônico:** É permitido o acesso remoto pelos Colaboradores ao correio eletrônico quando o mesmo estiver fora do ambiente da Moat Capital através da Internet.

**Responsabilidades e Forma de Uso de Correio Eletrônico:** É responsabilidade dos Colaboradores da Moat Capital o acesso, conteúdo de mensagens e uso relativo ao seu endereço de correio eletrônico.

Dessa forma, o Colaborador deve sempre se atentar antes de enviar o e-mail: (i) ao nível de sigilo do teor da mensagem; (ii) aos anexos; (iii) ao uso da opção "encaminhar" para não enviar mensagens anteriores sem necessidade; e (iv) os destinatários que vão receber a mensagem.

É proibido criar, copiar ou encaminhar mensagens ou imagens que: (i) contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza; (ii) façam parte de correntes de mensagens; (iii) incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física; (iv) possuam informação imprópria para o ambiente profissional; (v) sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros; (vi) possibilitem a realização de atividades ilegais; (vii) possam prejudicar a imagem da Moat Capital; e (viii) sejam incoerentes com o Código de Ética da Moat Capital.

**Cópias de Segurança do Correio Eletrônico:** Como forma de tornar a gestão segura, confiável e passível de auditoria, o e-mail corporativo da Moat Capital fica armazenado na nuvem em um provedor reconhecido.

**Armazenamento em Nuvem:** O armazenamento das Informações Confidenciais e quaisquer outros dados serão feitos na nuvem, de modo efetivo, de acordo com o disposto nas Resoluções

nº 4.658, de 26 de abril de 2018 e 4.752, de 26 de setembro de 2019 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

**Contratação de Terceiros para Serviços de Armazenamento na Nuvem:** A Moat Capital contrata o serviço de nuvem por ser um ambiente seguro para o armazenamento de dados. Outros serviços na nuvem podem ser considerados, sendo necessário aplicar os mesmos procedimentos aos provedores, como: (i) *Software as a Service* (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores; (ii) *Platform as a Service* (PaaS) – desenvolvimento, teste, uso e controle sobre softwares próprios; e (iii) *Infrastructure as a Service* (IaaS) – utilização e controles sobre softwares próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

**Testes de Intrusão:** São realizados testes de intrusão, interno e externo, pelo menos uma vez ao ano, nas camadas de rede com a finalidade de verificar possíveis ataques.

**Varredura de Vulnerabilidades:** As varreduras nas redes internas e externas da Moat Capital são realizadas periodicamente com o intuito de identificar eventuais vulnerabilidades. Uma vez identificadas a Moat Capital dará prioridade, realizando o devido tratamento de acordo com o seu nível de criticidade.

**Rastreabilidade:** Como forma de reconstruir eventos como: (i) autenticação de usuários; (ii) acesso à informações; e (iii) ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema, a Moat Capital implementa trilha de auditoria automatizada implantada para todos os componentes de sistema.

## VI. CONTINUIDADE DOS NEGÓCIOS

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

## VII. PLANO DE RESPOSTA

Caso ocorra o vazamento de Informações Confidenciais ou qualquer falha de segurança no sistema, a Moat Capital, deverá tomar as seguintes providencias:

**Área de Tecnologia da Informação e Tecnoqualify:** (i) verificação e auditoria dos acessos, bem como das informações potencialmente vazadas; (ii) eliminação dos aplicativos indesejados; (iii) varredura; (iv) reconstrução do sistema operacional e das redes; (v) restauração de dados provenientes do backup diário; e (vi) quaisquer outras medidas necessárias.

**Área de Compliance:** (i) elaboração de relatório com base na verificação e auditoria feita pela Área de Tecnologia da Informação e pela Tecnoqualify incluindo eventuais consequências reputacionais e jurídicas que a Moat Capital pode ter sofrido ou vir a sofrer; (ii) elaboração de notificação aos afetados, em caso de confirmação de vazamento de informações; e (iii) elaboração de planejamento de contenção de risco de liquidez em razão dos possíveis resgates de investimentos que a Moat Capital pode vir a sofrer.

Poderá ainda ser avaliada a necessidade de contratação de empresa especializada para combater o evento ocorrido, bem como eventuais respostas.

Todo evento será arquivado fisicamente na Moat Capital pelo período mínimo de 5 (cinco) anos.

## VIII. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. A presente Política poderá ainda ser alterada a qualquer tempo em razão de circunstâncias que demandam tal providência.