POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA COTA CAPITAL GESTORA DE ATIVOS

As diretrizes de Segurança da Informação e Cibernética da **COTA CAPITAL GESTORA DE ATIVOS** aderem-se integralmente ao comprometimento da alta administração e aos objetivos estratégicos dos negócios da organização e assegura o cumprimento das exigências normativas, de órgãos reguladores, de Compliance e requisitos legais de todo o ambiente da **COTA CAPITAL GESTORA DE ATIVOS**.

A **COTA CAPITAL GESTORA DE ATIVOS** trabalha com princípios que visam garantir a proteção da informação de nossos clientes, parceiros, terceiros, profissionais ou qualquer instituição ou pessoa que tenha relacionamento com a companhia, são eles:

Confidencialidade
Somente o usuário da informação, que esteja devidamente autorizado pelo Gestor da Informação, deve ter acesso às Informações respeitando os critérios de segregação de funções pré-definidos;

Integridade
Garante que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo Gestor da Informação;

Disponibilidade
Procura garantir que as Informações estejam sempre disponíveis para o Usuário da Informação;

Autenticidade
Garante a identidade de quem está enviando a Informação;

Esses pilares são a base para que os processos de Governança da Segurança da Informação e Cibernética sejam atendidos e controlados, de forma a:

- Estabelecer diretrizes para a classificação de dados e informações, por meio de critérios e restrições para acesso, processamento ou transmissão da informação confidencial, sensível ou restrita da **COTA CAPITAL GESTORA DE ATIVOS**, parceiros ou de seus clientes que não tenham sido autorizadas pelos responsáveis;
- Implementar procedimentos e controles para mitigação das vulnerabilidades, incidentes e riscos de segurança, sinalizar a saúde do ambiente e produzir planos de remediação e/ou contenção, geração de riscos de segurança, além de informações sobre a situação e estado dos ativos frente as preocupações, ameaças de acordo ao apetite à risco e às estratégias das Companhias, reduzindo assim as superfícies de ataques e os respectivos riscos associados;
- Realizar a gestão, identificação, resposta, tratamento e redução de incidentes de segurança da informação, assim como o monitoramento proativo, a detecção e a investigação de tais ocorrências, por meio dos serviços de inteligência (threat

intelligence) e ainda, comunicar e/ou compartilhar (quando aplicável e especialmente no caso de incidente relevante) as áreas envolvidas, os órgãos reguladores, parceiros de inteligência e entidades externas;

- Prover mecanismos de prevenção ao vazamento de dados e informações (Data Loss Prevention – DLP), para detecção de possíveis violações ou padrões de condutas que possam infringir regulamentos das Companhias;
- Disponibilizar mecanismos de proteção, por meio do monitoramento de atividades de endpoints, sensores e controles de proteção de hardware ou software, contra códigos maliciosos que uma vez executados possam se infiltrar ou causar danos nas redes ou ativos das Companhias;
- Prover diretrizes de utilização dos recursos de rede, ou em contexto mais abrangente, dos recursos computacionais, sejam estes ativos fixos e/ou dispositivos móveis, removíveis, visando as melhores práticas de manipulação, proteção, processamento, monitoração e compartilhamento de informações; POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA Áreas responsáveis: Segurança da Informação & Compliance Data: Setembro/2023 3
- Prover planos e subplanos (Impacto no Negócio, Continuidade Operacional, Recuperação de Negócios, Gerenciamento de Incidentes, Administração de Crises e Planos de Testes/Validações) de recuperação de serviços críticos para garantir a disponibilidade operacional e da continuidade de negócio, bem como, procedimentos operacionais que possam reduzir os impactos decorrentes da interrupção de serviços causada por desastres, crises, indisponibilidades, falhas, comprometimentos ou eventos relevantes de segurança;
- Gerenciar e monitorar via Controle de Acessos, sejam estes físicos e/ou lógicos, às informações e ativos bem como o seu armazenamento, compartilhamento e descarte, para que somente pessoas autorizadas possam utilizá-los e em conformidade com regras, permissões, perfis e/ou políticas corporativas;
- Estabelecer critérios seguros de uso e manutenção de credenciais, segredos, tokens e senhas no contexto de utilização dos sistemas corporativos;
- Dar ciência aos profissionais, usuários, prestadores de serviços, clientes e parceiros de que: o não é permitido remover controles de segurança ou aplicações utilizadas para o acesso das informações ou proteção, bem como prover alterações em ambiente produtivo sem prévia aprovação; o os meios de comunicação, equipamentos de acesso a sistemas de informações e infraestruturas complementares são de propriedade da Companhia e passíveis de monitoração, sendo que os acessos ao conteúdo da internet e uso de e-mail é de responsabilidade do profissional titular da conta, do prestador de serviço, cliente ou parceiro, estando sujeito à aplicação de leis, decretos e regulamentos governamentais vigentes; e o não é permitido o uso de qualquer recurso tecnológico ou informações proprietárias em ações ilegais e nem a instalação de recurso computacional não autorizado.

- Definir controles fundamentais para o ciclo de vida e desenvolvimento seguro de software, utilização de novas tecnologias que possam guiar projetos dentro do contexto software seguro;
- Ajudar no dimensionamento dos requisitos de segurança a partir de arquitetura de referência, uso de controles criptográficos e proteções necessárias de acordo com a complexidade e nível de segurança necessário para cada componente;
- Garantir que sistemas desenvolvidos internamente ou adquiridos de fornecedores atendam aos padrões de segurança e melhores-práticas definidos pelo mercado ou pelas necessidades de negócio;
- Estabelecer diretrizes para manutenção de cópias de segurança (backup e restore) de dados e informações para os repositórios e locais de armazenamento oficiais das Companhias, assim como regramentos para a retenção da informação e logging, em conformidade com os órgãos reguladores e questões legais vigentes;
- Divulgar continuamente em todos os níveis, esferas e para o maior público possível, interna e/ou externamente (aos clientes) quando aplicável, programas e ações de conscientização, treinamentos, aculturamento e prevenção em relação à temática de Segurança da Informação e Cibernética;
- Analisar, aprovar e classificar contratos, nos termos da legislação vigente e sob o **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA**;
- Suportar questões de risco oferecendo um modelo e processo de risco comum, integrado e contínuo de identificação, análise, avaliação, tratamento, revisão e comunicação dos riscos mapeados, a fim de proteger os ativos das companhias em avaliações e definições de controles que possam validar o escopo desta política no intuito de aferir o nível de segurança dos controles de segurança da informação, em atendimento às áreas demandantes (Auditoria Interna, Controles Internos e Compliance). *A violação de controle de segurança ou o não cumprimento das diretrizes é considerada infração e poderá implicar em medidas disciplinares (sanções) a serem validadas pelos departamentos de Recursos Humanos, Jurídico, Compliance e Segurança da Informação COTA CAPITAL GESTORA DE ATIVOS, conforme sua natureza e enquadramentos previstos nas leis vigentes.*

Asset Management Compan
COTA CAPITAL GESTORA DE ATIVOS
CNPJ - 19.969.164/0001-50

CEO (Chief Executive Officer
GABRIEL ALVES APOSTO
CPF – 460.760.228-09

Política de Segurança da Informação.pdf

Documento número #00f79ff4-cf4d-45a0-b398-0638ba3e386c

Hash do documento original (SHA256): a875e6b1fd6e9b1f89e2be140dfecef80ca8cb94c63d0e226b1aeb28941825be

Assinaturas

COTA CAPITAL F INVESTIMENTOS

CPF: 025.253.559-62

Assinou como parte em 23 mai 2026 às 20:49:18

GABRIEL ALVES APOSTO

Assinou como parte em 23 mai 2026 às 22:54:41

Log

23 mai 2026, 20:45:36	Operador com email atendimento@cotainvesting.com.br na Conta def73590-560b-4080-9abe-75f28f7da536 criou este documento número 00f79ff4-cf4d-45a0-b398-0638ba3e386c. Data limite para assinatura do documento: 22 de junho de 2026 (20:45). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
23 mai 2026, 20:48:35	Operador com email atendimento@cotainvesting.com.br na Conta def73590-560b-4080-9abe-75f28f7da536 alterou o processo de assinatura. Data limite para assinatura do documento: 01 de julho de 2026 (16:54).
23 mai 2026, 20:48:36	Operador com email atendimento@cotainvesting.com.br na Conta def73590-560b-4080-9abe-75f28f7da536 adicionou à Lista de Assinatura: adm@cotainvesting.com.br para assinar como parte, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF. Dados informados pelo Operador para validação do signatário: nome completo COTA CAPITAL F INVESTIMENTOS e CPF 025.253.559-62.
23 mai 2026, 20:48:36	Operador com email atendimento@cotainvesting.com.br na Conta def73590-560b-4080-9abe-75f28f7da536 adicionou à Lista de Assinatura: gabrielaposto@cotainvesting.com.br para assinar como parte, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo. Dados informados pelo Operador para validação do signatário: nome completo GABRIEL ALVES APOSTO.
23 mai 2026, 20:49:18	COTA CAPITAL F INVESTIMENTOS assinou como parte. Pontos de autenticação: Token via E-mail adm@cotainvesting.com.br. CPF informado: 025.253.559-62. IP: 189.58.150.73. Localização compartilhada pelo dispositivo eletrônico: latitude -23.60025249636013 e longitude -46.66216650145913. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1447.0 disponibilizado em https://app.clicksign.com.

23 mai 2026, 22:54:41	GABRIEL ALVES APOSTO assinou como parte. Pontos de autenticação: Token via E-mail gabrielaposto@cotainvesting.com.br. IP: 177.141.180.143. Componente de assinatura versão 1.1447.0 disponibilizado em https://app.clicksign.com.
23 mai 2026, 22:54:42	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 00f79ff4-cf4d-45a0-b398-0638ba3e386c.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 00f79ff4-cf4d-45a0-b398-0638ba3e386c, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.