TOTH CAPITAL

POLÍTICA DE SEGURANÇA CIBERNÉTICA

TOTH CAPITAL ASSET MANAGEMENT LTDA

NOVEMBRO de 2025

FICHA TÉCNICA

Títulos:	Política de Segurança Cibernética
Área:	Responsável: Compliance
Descrição da Política:	Manual que descreve as políticas, regras e procedimentos de controles internos da TOTH Capital Asset Management Ltda
Aplicação:	Todos os Colaboradores da TOTH Capital Asset Management Ltda
Tipo:	Política Institucional
Data de Aprovação:	28/11/2025
Criada por:	Compliance
Aprovada por:	Comitê Interno
Data de Publicação:	15/12/2025

TOTH CAPITAL ASSET MANAGEMENT LTDA

POLÍTICA DE SEGURANÇA CIBERNÉTICA
Data de Aprovação: 28/11/2025

POLÍTICA DE SEGURANÇA CIBERNÉTICA

REGRAS GERAIS

Todos que tenham acesso aos sistemas informáticos da TOTH Capital são responsáveis pelas precauções necessárias para esse processo. Todos devem salvaguardar as senhas e outros meios de acesso a sistemas e documentos.

A segurança cibernética é um dos principais patrimônios de uma Instituição e a segurança dos dados deve ser um esforço contínuo para manutenção e proteção desse patrimônio.

As senhas são de uso individual e não devem ser divulgadas ou compartilhadas com outras pessoas sob nenhuma hipótese, sendo de inteira responsabilidade do detentor o zelo pela guarda e uso correto dela. Deve ser evitada a exposição de documentos de clientes ou de caráter confidencial.

Todos os documentos devem permanecer trancados em local seguro, quando não estiverem sendo manuseados.
Três princípios são essenciais no processo de Segurança Cibernética:

• Confidencialidade – Garantir que informações relevantes sejam acessadas somente por áreas e pessoas autorizadas;
• Integridade – garantir a veracidade e qualidade das informações fornecidas, evitando modificações indevidas, propositais ou não;
• Disponibilidade – Garantir o acesso de pessoas autorizadas à informação.

TREINAMENTO

Todos os colaboradores deverão ter acesso a política e fazer o treinamento de Segurança Cibernética, para terem ciência dos seus deveres, e dos procedimentos a serem aplicados para manter a segurança cibernética da empresa.

AVALIAÇÃO DE RISCOS

A TOTH Capital deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. A gestora segue, em sua Política, o Código ANBIMA de Segurança Cibernética que definiu os ataques mais comuns de criminosos cibernéticos (cybercriminals) sendo os

seguintes:

a) Malware (e.g. vírus, cavalo de troia, spyware e ransomware);
b) Engenharia Social;
c) Pharming;
d) Phishing scam;
e) Vishing;
f) Smishing;
g) Acesso pessoal;
h) Ataques de DDoS e botnets; e
i) Invasões (advanced persistent threats).

AÇÕES DE PROTEÇÃO E PREVENÇÃO, A FIM DE MITIGAR OS RISCOS IDENTIFICADOS

A TOTH Capital 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 TOTH Capital trabalha com o princípio de que a 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 TOTH Capital 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 TOTH Capital conta com recursos *anti-malware* em estações e servidores de rede, como antivírus e firewalls pessoais. Da mesma maneira, monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas. A TOTH Capital realiza, também, backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Continuidade do Negócio.

Manutenção trimestral de todos os hardwares e Backup diário, realizado na nuvem. Sem prejuízo dos testes realizados na forma do roteiro para a realização de testes para a Verificação de Aderência aos Documentos Internos da Gestora, a Gestora realizará simulações de ataques e respostas que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da Gestora, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

O backup de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da Gestora, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência. As rotinas de backup são periodicamente monitoradas.

MECANISMOS DE SUPERVISÃO PARA CADA RISCO

Diretrizes de Segurança da Informação: Adoção de Comportamento Seguro, independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da TOTH Capital e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

a) Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;
b) Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das Informações Sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;
c) Todo tipo de acesso aos dados e informações da TOTH Capital, em especial as Informações Sigilosas, que não forem expressamente autorizadas são proibidas;
d) Assuntos relacionados ao desempenho de atividades e funções na Gestora não devem ser discutidos em ambientes públicos ou em áreas expostas (e.g. meios de transporte, locais públicos, encontros sociais);
e) As senhas de acesso do Colaborador aos sistemas da Gestora são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;
f) Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;
g) Somente softwares homologados e previamente aprovados pela TOTH Capital podem ser instalados e usados nas estações de trabalho, o que deve ser feito com exclusividade pela equipe de serviços de informática da Gestora;
h) Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da Gestora;
i) Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter Informações Sigilosas. Portanto, não podem ser parciais ou totalmente divulgadas, usadas ou reproduzidas sem o consentimento prévio do remetente ou do autor. Toda e qualquer divulgação, uso e/ou reprodução não expressamente autorizada é proibida. O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela TOTH Capital. 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 TOTH Capital Asset em risco.
j) Caso o colaborador identifique ou suspeite que alguma informação confidencial foi vazada, ou que houve algum tipo de invasão a algum dispositivo que contenha informações da empresa, este deverá informar imediatamente o departamento de Compliance, para que sejam tomadas as devidas ações de contenção, para minimizar o possível problema.

PLANO DE RESPOSTA A INCIDENTES

Havendo indícios ou de suspeita fundamentada, a empresa 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 Ética e Conduta. Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão 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, ainda que sumariamente, constar no Relatório de Controles Internos.

São Paulo, 28 de Novembro de 2025.

TOTH Capital Asset Management Ltda

Contato: LUCAS COSLOSKI IAMONDI | (11) 9753239878 | LUCAS.IAMONDI@TOTHCAPITAL.COM.BR