TRÍTONO
CAPITAL

# POLÍTICA DE SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS

**TRÍTONO CAPITAL GESTÃO DE RECURSOS LTDA.**

**CNPJ:** 62.955.469/0001-31
**Endereço:** Rua Potiguar Medeiros, S/N, Pinheiros, São Paulo/SP, CEP 05422-100
**Versão:** 1.0
**Data de Aprovação:** novembro de 2025
**Responsável:** Diretoria

**CONTROLE DE VERSÕES:**

| Versão | Data | Responsável | Aprovação |
|---|---|---|---|
| 1.0 | Novembro/2025 | Diretoria | Diretoria |

**SUMÁRIO**



## 1. INTRODUÇÃO

A Política de Segurança Cibernética e Proteção de Dados da Trítono Capital Gestão de Recursos Ltda. ("Trítono Capital" ou "Gestora") foi desenvolvida para abordar os crescentes desafios de segurança no ambiente digital, reconhecendo que a proteção dos ativos digitais e a salvaguarda das informações confidenciais são fundamentais para a continuidade dos negócios e para a manutenção da confiança dos investidores e parceiros.

O panorama da segurança cibernética tem evoluído rapidamente, apresentando desafios cada vez mais complexos para as organizações do mercado financeiro. A Gestora reconhece que, como gestora especializada em Fundos de Investimento em Participações, lida com informações altamente sensíveis sobre investidores, empresas investidas e estratégias de investimento, tornando a segurança cibernética uma prioridade estratégica.

Este documento foi cuidadosamente desenvolvido para abordar os riscos emergentes no cenário de segurança cibernética, fornecendo diretrizes claras e procedimentos robustos para mitigar ameaças e promover práticas seguras no ambiente digital. O objetivo é fortalecer a resiliência da organização diante dos

desafios crescentes e garantir que todas as áreas estejam preparadas para enfrentar os riscos cibernéticos de forma eficaz.

Esta política trata das regras e procedimentos que visam proteger os sistemas de informação, prevenir ataques cibernéticos, gerenciar incidentes de segurança e promover uma cultura de conscientização e responsabilidade compartilhada. Também aborda as melhores práticas e os padrões reconhecidos internacionalmente para a segurança cibernética, garantindo que as políticas estejam alinhadas às últimas recomendações do setor.

É importante ressaltar que a segurança cibernética é uma responsabilidade de todos os colaboradores da Gestora. Cada pessoa desempenha um papel fundamental na proteção dos ativos digitais e no fortalecimento da postura de segurança. A Gestora está comprometida em manter um ambiente seguro e confiável, investindo continuamente em recursos e tecnologias adequadas para mitigar os riscos cibernéticos.

## 2. OBJETIVOS E ESCOPO

### 2.1. Objetivos

Esta política tem os seguintes objetivos principais:

**Proteção de Informações:** Assegurar a confidencialidade, integridade e disponibilidade das informações da Gestora, seus investidores e empresas investidas.

**Conformidade Regulatória:** Garantir o cumprimento da Lei Geral de Proteção de Dados (LGPD), regulamentações da CVM e demais normas aplicáveis.

**Gestão de Riscos:** Identificar, avaliar e mitigar riscos cibernéticos que possam impactar as operações da Gestora.

**Continuidade de Negócios:** Assegurar a continuidade das operações críticas em caso de incidentes de segurança.

**Cultura de Segurança:** Promover uma cultura organizacional que valorize e pratique a segurança da informação.

### 2.2. Escopo

Esta política aplica-se a:

**Pessoas:** Todos os colaboradores, administradores, estagiários, terceirizados e prestadores de serviços da Gestora.

**Informações:** Todas as informações em formato digital ou físico sob responsabilidade da Gestora.

**Sistemas:** Todos os sistemas de informação, equipamentos e infraestrutura tecnológica utilizados pela Gestora.

**Processos:** Todos os processos de negócio que envolvam o tratamento de informações.

**Localização:** Todas as instalações da Gestora e locais onde suas atividades são desenvolvidas.

### 2.3. Princípios Fundamentais

**Confidencialidade:** As informações devem ser acessíveis apenas a pessoas autorizadas.

**Integridade:** As informações devem ser precisas, completas e protegidas contra alterações não autorizadas.

**Disponibilidade:** As informações e sistemas devem estar disponíveis quando necessários.

**Autenticidade:** A origem das informações deve ser verificável e confiável.

**Não Repúdio:** As ações realizadas devem ser rastreáveis e não negáveis.

## 3. DEFINIÇÕES

Para os fins desta política, aplicam-se as seguintes definições:

**Ativo de Informação:** Qualquer informação ou sistema que tenha valor para a Gestora.

**Ameaça:** Qualquer circunstância ou evento com potencial de causar danos aos ativos de informação.

**Vulnerabilidade:** Fraqueza em um ativo ou controle que pode ser explorada por uma ameaça.

**Risco:** Probabilidade de uma ameaça explorar uma vulnerabilidade e causar impacto.

**Incidente de Segurança:** Evento que compromete ou pode comprometer a segurança da informação.

**Dados Pessoais:** Informações relacionadas a pessoa natural identificada ou identificável.

**Dados Pessoais Sensíveis:** Dados sobre origem racial, convicções religiosas, opiniões políticas, saúde, vida sexual, dados genéticos ou biométricos.

**Tratamento:** Toda operação realizada com dados pessoais.

**Controlador:** Pessoa natural ou jurídica que toma decisões sobre o tratamento de dados pessoais.

**Operador:** Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

**Malware:** Software malicioso projetado para danificar ou obter acesso não autorizado a sistemas.

**Phishing:** Técnica de engenharia social para obter informações confidenciais.

**Ransomware:** Tipo de malware que criptografa dados e exige pagamento para descriptografia.

## 4. RESPONSABILIDADES

### 4.1. Diretoria

A Diretoria é responsável por:

- Aprovar e revisar esta política
- Definir a estratégia de segurança cibernética
- Assegurar recursos adequados para segurança
- Supervisionar a gestão de riscos cibernéticos
- Tomar decisões sobre incidentes críticos
- Comunicar-se com stakeholders sobre questões de segurança

### 4.2. Diretor de Compliance

O Diretor de Compliance é responsável por:

- Implementar e manter esta política
- Coordenar atividades de segurança cibernética
- Monitorar conformidade com regulamentações
- Gerenciar incidentes de segurança
- Treinar colaboradores sobre segurança
- Elaborar relatórios de segurança
- Coordenar com prestadores de serviços de TI

### 4.3. Diretor Presidente

O Diretor Presidente é responsável por:

- Apoiar a implementação da política
- Assegurar que decisões de negócio considerem aspectos de segurança
- Comunicar-se com investidores sobre questões de segurança
- Participar da gestão de crises cibernéticas

### 4.4. Colaboradores

Todos os colaboradores devem:

- Conhecer e cumprir esta política
- Proteger informações confidenciais
- Usar sistemas de forma segura
- Reportar incidentes de segurança

- Participar de treinamentos obrigatórios
- Manter senhas seguras
- Ser vigilantes contra ameaças cibernéticas

### 4.5. Prestadores de Serviços

Os prestadores de serviços devem:
- Cumprir requisitos de segurança contratuais
- Implementar controles adequados
- Reportar incidentes que afetem a Gestora
- Permitir auditorias de segurança
- Manter confidencialidade de informações

## 5. GOVERNANÇA DE SEGURANÇA

### 5.1. Estrutura de Governança

A governança de segurança cibernética da Gestora é estruturada da seguinte forma:

**Nível Estratégico:** Diretoria define estratégia e aprova políticas.

**Nível Tático:** Diretor de Compliance coordena implementação e monitoramento.

**Nível Operacional:** Colaboradores executam controles e procedimentos diários.

### 5.2. Comitê de Segurança

Quando necessário, a Gestora pode constituir comitê temporário de segurança para tratar de questões específicas, composto por:
- Diretor de Compliance (coordenador)
- Diretor Presidente
- Representantes de prestadores de TI
- Outros especialistas conforme necessário

### 5.3. Políticas e Procedimentos

A Gestora mantém conjunto abrangente de políticas e procedimentos de segurança, incluindo:

- Esta política geral de segurança cibernética
- Procedimentos específicos por área
- Guias de boas práticas
- Planos de resposta a incidentes
- Procedimentos de backup e recuperação

### 5.4. Gestão de Riscos

**Identificação:** Identificação sistemática de riscos cibernéticos.

**Avaliação:** Análise de probabilidade e impacto dos riscos.

**Tratamento:** Implementação de controles para mitigar riscos.

**Monitoramento:** Acompanhamento contínuo da efetividade dos controles.

## 6. GESTÃO DE ATIVOS DE INFORMAÇÃO

### 6.1. Classificação de Informações

As informações da Gestora são classificadas conforme seu nível de sensibilidade:

**Público:** Informações que podem ser divulgadas publicamente sem restrições.

**Interno:** Informações de uso interno da Gestora, não destinadas ao público externo.

**Confidencial:** Informações sensíveis que podem causar danos se divulgadas inadequadamente.

**Restrito:** Informações altamente sensíveis com acesso limitado a pessoas específicas.

### 6.2. Tratamento por Classificação

**Informações Públicas:** - Podem ser divulgadas sem restrições – Armazenamento em sistemas padrão – Backup conforme procedimentos normais

**Informações Internas:** - Acesso limitado a colaboradores – Controles básicos de acesso – Cuidados na comunicação externa

**Informações Confidenciais:** - Acesso baseado em necessidade professional – Controles rigorosos de acesso – Criptografia quando apropriado – Acordos de confidencialidade

**Informações Restritas:** - Acesso limitado a pessoas específicas – Controles máximos de segurança – Criptografia obrigatória – Logs detalhados de acesso – Aprovação para cada acesso

### 6.3. Inventário de Ativos

A Gestora mantém inventário atualizado de seus ativos de informação, incluindo:

- Sistemas de informação
- Bases de dados
- Equipamentos de TI
- Documentos físicos e digitais
- Aplicações e software
- Serviços de terceiros

### 6.4. Propriedade e Custódia

**Proprietário do Ativo:** Responsável pela classificação e autorização de acesso.

**Custodiante:** Responsável pela implementação de controles e proteção física/lógica.

**Usuário:** Responsável pelo uso adequado conforme políticas estabelecidas.

## 7. CONTROLES DE ACESSO

### 7.1. Gestão de Identidades

**Criação de Contas:** - Processo formal de solicitação - Aprovação por responsável autorizado - Princípio do menor privilégio - Documentação adequada

**Manutenção de Contas:** - Revisão periódica de acessos - Atualização conforme mudanças de função - Desativação de contas desnecessárias - Monitoramento de atividades

**Exclusão de Contas:** - Desativação imediata no desligamento - Transferência de responsabilidades - Recuperação de equipamentos - Revogação de certificados

### 7.2. Autenticação

**Senhas:** - Complexidade mínima exigida - Alteração periódica obrigatória - Proibição de reutilização - Armazenamento seguro

**Autenticação Multifator:** - Obrigatória para sistemas críticos - Combinação de fatores diferentes - Tokens ou aplicativos autenticadores - Backup de métodos de autenticação

### 7.3. Autorização

**Perfis de Acesso:** - Definição baseada em funções - Segregação de responsabilidades - Aprovação por níveis hierárquicos - Documentação de justificativas

**Controles de Acesso:** - Implementação técnica de restrições - Monitoramento de tentativas de acesso - Logs detalhados de atividades - Alertas para atividades suspeitas

### 7.4. Acesso Remoto

**VPN Corporativa:** - Conexão criptografada obrigatória - Autenticação forte - Monitoramento de conexões - Políticas de uso aceitável

**Dispositivos Móveis:** - Configuração de segurança obrigatória - Criptografia de dados - Possibilidade de limpeza remota - Controles de aplicações

# 8. SEGURANÇA DE REDES E SISTEMAS

## 8.1. Arquitetura de Segurança

**Segmentação de Rede:** - Separação de ambientes por criticidade - Controles de tráfego entre segmentos - Monitoramento de comunicações - Isolamento de sistemas críticos

**Perímetro de Segurança:** - Firewall com regras restritivas - Sistema de detecção de intrusão - Filtragem de conteúdo web - Proteção contra malware

## 8.2. Proteção de Endpoints

**Antivírus/Anti-malware:** - Instalação obrigatória em todos os equipamentos - Atualizações automáticas - Varreduras regulares - Quarentena de arquivos suspeitos

**Configuração Segura:** - Hardening de sistemas operacionais - Desabilitação de serviços desnecessários - Atualizações de segurança regulares - Controles de instalação de software

## 8.3. Gestão de Vulnerabilidades

**Identificação:** - Varreduras regulares de vulnerabilidades - Monitoramento de alertas de segurança - Análise de logs de segurança - Testes de penetração periódicos

**Correção:** - Priorização baseada em criticidade - Cronograma de aplicação de patches - Testes antes da implementação - Verificação de efetividade

## 8.4. Backup e Recuperação

**Estratégia de Backup:** - Backup regular de dados críticos - Cópias em locais diferentes - Testes regulares de restauração - Criptografia de backups

**Plano de Recuperação:** - Procedimentos documentados - Tempos de recuperação definidos - Responsabilidades claras - Testes periódicos do plano

## 9. PROTEÇÃO DE DADOS PESSOAIS

### 9.1. Conformidade com LGPD

A Gestora atua como controladora de dados pessoais e implementa medidas para conformidade com a Lei Geral de Proteção de Dados:

**Bases Legais:** - Identificação de bases legais para cada tratamento - Documentação de justificativas - Revisão periódica de adequação - Comunicação clara aos titulares

**Direitos dos Titulares:** - Procedimentos para exercício de direitos - Canais de comunicação adequados - Prazos de resposta estabelecidos - Treinamento de colaboradores

### 9.2. Princípios de Proteção

**Finalidade:** Tratamento para propósitos legítimos e específicos.

**Adequação:** Compatibilidade com finalidades informadas.

**Necessidade:** Limitação ao mínimo necessário.

**Livre Acesso:** Garantia de consulta facilitada sobre tratamento.

**Qualidade dos Dados:** Exatidão, clareza e atualização.

**Transparência:** Informações claras sobre tratamento.

**Segurança:** Medidas técnicas e administrativas adequadas.

**Prevenção:** Adoção de medidas preventivas.

**Não Discriminação:** Impossibilidade de tratamento discriminatório.

**Responsabilização:** Demonstração de conformidade.

### 9.3. Medidas de Segurança

**Técnicas:** - Criptografia de dados sensíveis - Controles de acesso granulares - Anonimização quando possível - Pseudonimização de dados

**Administrativas:** - Políticas e procedimentos claros - Treinamento regular de colaboradores - Contratos com cláusulas de proteção - Auditorias regulares

**Físicas:** - Controles de acesso a instalações - Armazenamento seguro de documentos - Descarte seguro de informações - Proteção de equipamentos

### 9.4. Gestão de Incidentes com Dados Pessoais

**Detecção:** - Monitoramento contínuo - Canais de reporte - Investigação de suspeitas - Documentação de evidências

**Resposta:** - Contenção imediata - Avaliação de impacto - Comunicação à ANPD quando necessário - Notificação aos titulares quando aplicável

## 10. GESTÃO DE INCIDENTES

### 10.1. Definição de Incidentes

São considerados incidentes de segurança:

- Acesso não autorizado a sistemas ou dados
- Vazamento de informações confidenciais
- Ataques de malware ou ransomware
- Indisponibilidade de sistemas críticos
- Tentativas de fraude ou phishing
- Perda ou roubo de equipamentos
- Violações de políticas de segurança

### 10.2. Processo de Gestão

**Detecção e Reporte:** - Canais múltiplos de comunicação - Reporte imediato obrigatório - Preservação de evidências - Documentação inicial

**Análise e Classificação:** - Avaliação de severidade - Classificação por tipo de incidente - Determinação de impacto - Acionamento de equipe apropriada

**Contenção:** - Ações imediatas para limitar danos - Isolamento de sistemas afetados - Preservação de evidências - Comunicação com stakeholders

**Erradicação:** - Remoção da causa do incidente - Correção de vulnerabilidades - Limpeza de sistemas afetados - Implementação de melhorias

**Recuperação:** - Restauração de sistemas - Verificação de integridade - Monitoramento intensificado - Retorno às operações normais

**Lições Aprendidas:** - Análise pós-incidente - Identificação de melhorias - Atualização de procedimentos - Treinamento adicional

### 10.3. Equipe de Resposta

**Coordenador:** Diretor de Compliance

**Membros:** - Diretor Presidente - Prestadores de serviços de TI - Consultores externos quando necessário - Outros especialistas conforme o tipo de incidente

### 10.4. Comunicação

**Interna:** - Notificação imediata à Diretoria - Comunicação com colaboradores afetados - Atualizações regulares sobre status - Relatórios de progresso

**Externa:** - Comunicação com autoridades quando exigido - Notificação a investidores quando relevante - Coordenação com prestadores de serviços - Comunicação com mídia se necessário

## 11. CONTINUIDADE DE NEGÓCIOS

### 11.1. Integração com PCN

Esta política integra-se com o Plano de Continuidade de Negócios da Gestora, assegurando que aspectos de segurança cibernética sejam considerados em cenários de contingência.

### 11.2. Sistemas Críticos

**Identificação:** - Mapeamento de sistemas essenciais - Análise de dependências - Avaliação de impacto de indisponibilidade - Priorização para recuperação

**Proteção:** - Controles de segurança reforçados - Backup frequente e testado - Redundância quando apropriado - Monitoramento intensificado

### 11.3. Recuperação de Desastres

**Estratégia:** - Definição de objetivos de recuperação - Procedimentos de ativação - Recursos alternativos identificados - Testes regulares de procedimentos

**Implementação:** - Equipes de recuperação designadas - Comunicação coordenada - Verificação de integridade - Retorno gradual às Operações

## 12. TREINAMENTO E CONSCIENTIZAÇÃO

### 12.1. Programa de Treinamento

**Treinamento Inicial:** - Obrigatório para todos os novos colaboradores - Cobertura de políticas e procedimentos - Casos práticos e simulações - Avaliação de conhecimento

**Treinamento Contínuo:** - Atualizações regulares sobre ameaças - Simulações de phishing - Workshops sobre boas práticas - Treinamento específico por função

### 12.2. Conscientização

**Campanhas:** - Comunicações regulares sobre segurança - Alertas sobre novas ameaças - Dicas de segurança - Reconhecimento de boas práticas
**Materiais:** - Guias de boas práticas - Vídeos educativos - Cartazes e lembretes - Portal de segurança interno

### 12.3. Avaliação de Efetividade

**Métricas:** - Taxa de participação em treinamentos - Resultados de simulações - Número de incidentes reportados - Feedback dos participantes

**Melhoria:** - Análise de resultados - Ajustes no programa - Novos métodos de treinamento - Personalização por audiência

## 13. MONITORAMENTO E AUDITORIA

### 13.1. Monitoramento Contínuo

**Sistemas de Monitoramento:** - Logs de segurança centralizados - Alertas automatizados - Dashboards de segurança - Análise de comportamento

**Indicadores:** - Tentativas de acesso não autorizado - Atividades suspeitas - Performance de controles - Conformidade com políticas

### 13.2. Auditoria de Segurança

**Auditoria Interna:** - Revisões periódicas de controles - Testes de efetividade - Verificação de conformidade - Relatórios de achados

**Auditoria Externa:** - Avaliações independentes - Testes de penetração - Certificações de segurança - Validação de controles

### 13.3. Métricas e Relatórios

**Métricas de Segurança:** - Número de incidentes por período - Tempo de detecção e resposta - Taxa de conformidade - Efetividade de treinamentos

**Relatórios:** - Relatórios mensais de segurança - Relatórios de incidentes - Relatórios de auditoria - Apresentações para Diretoria

## 14. DISPOSIÇÕES GERAIS

### 14.1. Vigência

Esta política entra em vigor na data de sua aprovação pela Diretoria e permanece válida até sua revogação ou substituição por versão atualizada.

### 14.2. Atualizações

Esta política será revisada anualmente ou sempre que houver:

- Mudanças na regulamentação
- Evolução das ameaças cibernéticas
- Incidentes significativos
- Mudanças na infraestrutura
- Feedback de auditorias

### 14.3. Integração com Outras Políticas

Esta política deve ser lida em conjunto com:

- Política de Segregação de Atividades e Confidencialidade
- Plano de Continuidade de Negócios
- Manual de Compliance
- Código de Ética e Conduta
- Outras políticas internas relevantes

### 14.4. Conformidade

O cumprimento desta política é obrigatório para todos os colaboradores e prestadores de serviços. Violações podem resultar em:

- Medidas disciplinares
- Rescisão de contratos
- Ações legais quando apropriado
- Comunicação a autoridades

### 14.5. Melhoria Contínua

A Gestora compromete-se com a melhoria contínua de sua postura de segurança cibernética, incorporando:

- Lições aprendidas de incidentes
- Melhores práticas de mercado
- Novas tecnologias de segurança
- Feedback de stakeholders

### 14.6. Suporte e Recursos

A Gestora disponibiliza recursos adequados para implementação desta política, incluindo:

- Tecnologias de segurança apropriadas
- Treinamento regular de colaboradores
- Consultoria especializada quando necessário
- Investimentos em infraestrutura

### 14.7. Casos Omissos

Situações não previstas nesta política devem ser submetidas ao Diretor de Compliance para análise e orientação, sempre considerando os princípios de segurança e proteção estabelecidos.

### 14.8. Responsabilidade Compartilhada

A segurança cibernética é responsabilidade de todos na Gestora. Cada colaborador deve contribuir para a proteção dos ativos de informação e para a manutenção de um ambiente seguro e confiável.

**Aprovado pela Diretoria da Trítono Capital Gestão de Recursos Ltda.**
**São Paulo, Novembro de 2025**

**Daniel Teruo Famano**
Diretor Presidente

**Guilherme Maitto Caputo**
Diretor de Compliance