# Política de Segurança da Informação e de Segurança Cibernética

Quadrante INVESTIMENTOS

2020

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE SEGURANÇA CIBERNÉTICA DA QUADRANTE INVESTIMENTOS**

## 1. INTRODUÇÃO

A Quadrante Investimentos tem na informação um dos principais bens de sua empresa. Todo o conteúdo dos dados armazenados e que circulam em seu sistema deve respeitar a normatização em vigor e os preceitos de segurança estabelecidos pela instituição.

## 2. OBJETIVO

A presente Política de Segurança da Informação e de Segurança Cibernética tem por objetivo garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da organização, dos clientes e do público em geral, bem como assegurar uma pronta e imediata resposta a eventuais incidentes relacionados à segurança cibernética.

## 3. ABRANGÊNCIA

Esta Política deve ser observada por todas as áreas e colaboradores da Quadrante Investimentos, bem como todos aqueles que mantém relação profissional com a empresa, atendendo-se os padrões éticos e legais estabelecidos.

## 4. PRINCÍPIOS

São princípios que norteiam a Política de Segurança da Informação e de Segurança Cibernética da Quadrante Investimentos:

a) **Confidencialidade**: assegurar que as informações que estão sob a responsabilidade da empresa e seus colaboradores seja de uso exclusivo das pessoas autorizadas, assim como sejam utilizadas unicamente ao fim a que se destinam;

b) **Integridade**: preservar a integridade do conteúdo das informações mantidas sob a guarda da empresa, permitindo assegurar a credibilidade dos dados que circularão pela rede, protegendo a empresa contra o vazamento de informações e fraudes;

c) **Disponibilidade**: assegurar aos colaboradores e pessoas autorizadas o acesso a informações, possibilitando tratá-las de modo ético e em conformidade com os ditames desta Política e das normas legais.

## 5. ESCOPO REGULATÓRIO CONSIDERADO

A presente Política está em conformidade com as melhores práticas de mercado, notadamente:

- Instrução CVM nº 558, de 26 de março de 2015 ("ICVM 558");
- Código ANBIMA de Melhores Práticas para a Administração de Recursos de Terceiros ("Código ANBIMA ART"); e,
- Guia de Cibersegurança da ANBIMA, de 06 de dezembro de 2017.

## 6. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

A Quadrante Investimentos estabeleceu os seguintes controles e procedimentos de Segurança da Informação:

### 6.1. Política de proteção de informações e dados

A Quadrante tem dever ético, moral e profissional de manter sigilo absoluto sobre as informações dos clientes. Sendo assim, é terminantemente proibido comentar fora das instalações da Quadrante nomes de clientes ou quaisquer assuntos relacionados aos mesmos. Colaboradores da Quadrante, ao se relacionarem com colaboradores de outras áreas ou departamentos, devem assumir a mesma postura mencionada acima.

Quaisquer materiais gerados pela Quadrante bem como todos os dados e informações em geral, que deram suporte aos mesmos, devem também obedecer a política de sigilo absoluto. Sendo assim, é terminantemente proibido passar adiante informações ou opiniões obtidas na Quadrante ou no contato com membros de sua equipe. Da mesma maneira é terminantemente proibido enviar, utilizando-se de qualquer meio, materiais gerados pela Quadrante bem como todos os dados e informações em geral, que deram suporte aos mesmos

Sendo assim, todos os colaboradores da Quadrante devem assinar o "Termo de Confidencialidade", que atesta a total concordância com a presente política.

### 6.2. Confidencialidade de Informações

Com o objetivo de resguardar a privacidade de informações pessoais ou financeiras dos clientes, prevalecerá, em regra e em qualquer situação de dúvida, o caráter sigiloso de dados, informações, comunicações, saldos, posições e qualquer outro tipo de informações relativas a clientes que não sejam sabidamente de conhecimento público.

Os Colaboradores da Quadrante devem preservar a confidencialidade de qualquer informação relativa a clientes, obtida no desenvolvimento das atividades relacionadas à Quadrante, de caráter

pessoal ou profissional, mesmo após o término do vínculo com a Quadrante. A não observância da confidencialidade estará sujeita à apuração de responsabilidades nas esferas cível e criminal.

A revelação dessas informações a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada aos sócios da Quadrante, para que estes decidam sobre a forma mais adequada para tal revelação.

Tendo em vista a alta especialização da atividade desenvolvida pela Quadrante, assim como os princípios que regem o mercado de valores mobiliários, é absolutamente vedada a revelação de carteiras e estratégias de investimento de todo e qualquer produto analisado, administrados e/ou gerido pela Quadrante a qualquer pessoa ou instituição fora da Quadrante, seja da imprensa, de círculo pessoal de convívio, de ligação imediata de parentesco ou de estado civil. A não observância deste item estará sujeita à apuração de responsabilidades nas esferas cível e criminal.

### 6.3. Acesso à informação privilegiada

Considera-se informação privilegiada qualquer informação relevante a respeito de qualquer empresa, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada, em decorrência da relação profissional ou pessoal mantida com um cliente, com colaboradores de empresas analisadas ou investidas ou com terceiros, ou da condição de funcionário.

Exemplos de informações privilegiadas: informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, e qualquer outro fato que seja objeto de um acordo de confidencialidade firmado por uma empresa com a Quadrante ou com terceiros.

As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

Quem tiver acesso a uma informação privilegiada deverá divulgá-la imediatamente ao Comitê de Ética, composto pelos sócios da Quadrante, não devendo divulgá-la a ninguém, nem mesmo a outros integrantes da Quadrante, profissionais de mercado, amigos e parentes, e nem a utilizar, seja em benefício próprio ou de terceiros.

Caso haja dúvida sobre o caráter privilegiado da informação, aquele que a ela teve acesso deve imediatamente relatar tal fato ao Comitê de Ética. Todo aquele que tenha acesso a uma informação privilegiada deverá restringir ao máximo a circulação de documentos e arquivos que contenham essa informação.

### 6.4. Política de acesso ao Servidor e à Internet

A rotina diária de utilização das estações de trabalho (computadores) que dão acesso ao servidor da Quadrante está submetida a práticas de proteção de informações e dados.

Cada colaborador da Quadrante possui um “nome de usuário” e “senha” que dão acesso ao servidor. Será solicitada a criação de uma senha pessoal (que não deve ser divulgada para outras pessoas) na primeira vez que o servidor é acessado. Por motivo de segurança a senha deverá ser alterada periodicamente, conforme solicitação do sistema (qualquer dúvida solicite auxílio ao Setor de TI). A senha também é utilizada para desbloquear a estação de trabalho em caso de inatividade por mais de dez minutos. Os colaboradores, caso venham a se ausentar de suas mesas, devem bloquear as suas respectivas estações de trabalho através do seguinte procedimento: pressionar simultaneamente as teclas <Ctrl+Alt+Del> e selecionar a função “Bloquear computador”.

O acesso à internet, dado o seu risco de “infecção” de toda a rede da Quadrante e ao poder de dispersão de seus colaboradores, deve obedecer as seguintes regras: (i) somente sejam acessados sites que tenham relação direta com as atividades da Quadrante; (ii) é proibido baixar arquivos com extensão “zip” e executáveis, a não ser que o Setor de TI, após solicitação via e-mail, autorize; (iii) e-mails de fonte desconhecida ou suspeitos não devem ser abertos e o Setor de TI deve ser imediatamente comunicado.

### 6.5. Política de utilização de telefonia e atendimento telefônico

A Quadrante adota uma política de racionalização no uso da telefonia, com a premissa básica de que os telefones devem ser utilizados para assuntos que tenham relação direta com as atividades da Quadrante. Logicamente os colaboradores podem receber e fazer ligações pessoais, contudo a orientação é que isto seja feito com moderação e bom senso, o que inclui evitar ligações longas ou em quantidade excessiva, ligações para celulares ou interurbanos (caso seja necessário enviar solicitação, via e-mail, para o Setor de TI) que poderá autorizar a ligação.

### 6.6. Controle de Acessos

Todos os acessos dos colaboradores a sistemas que exijam “login” e “senha” estão mapeados, com a informação de quem pode acessar qual sistema.

Em casos específicos, tais como a menor suspeita de irregularidade nos acessos ou de “invasão” aos servidores ou máquinas da Quadrante Investimentos, a Diretoria de Compliance exigirá a troca imediata de senha para todos os sistemas por todos os respectivos usuários.

As violações ou desvio de finalidade quanto ao acesso ao sistema serão investigadas pela área técnica, a fim de sejam tomadas as medidas necessárias com o intuito de corrigir a falha ou reestruturar o processo.

#### 6.6.1. Acesso a informações confidenciais

Somente os diretores estatutários e pessoas autorizadas podem ter acesso a informações confidenciais na Quadrante.

Considera-se pessoas autorizadas o colaborador que em razão da área que exerce a sua atividade, necessita ter acessos a dados confidenciais da empresa e de seus clientes.

São considerados ainda pessoas autorizadas aquelas que participem do processo de decisão de investimentos ou do processo de distribuição de cotas de fundos de investimentos.

Todo o documento que contenha informação confidencial deverá ser armazenado em local seguro e de acesso restrito, cabendo ao colaborador que se utiliza das informações proteger o seu conteúdo, podendo ser responsabilizado pelo vazamento daquela informação ainda que involuntariamente.

**6.6.2. Acesso remoto a informações confidenciais**

Através da tecnologia de "armazenamento em nuvem" (também conhecida por "cloud computing"), os colaboradores da Quadrante Investimentos têm condições de acessar arquivos da rede de forma remota, isto é, de locais diversos do local de trabalho.

Todavia, no que se refere a informações confidenciais, somente os diretores estatutários e as pessoas autorizadas poderão acessar remotamente os arquivos que contenham conteúdo de natureza confidencial.

**6.6.3. Rastreamento de acesso às informações confidenciais**

O acesso ao sistema da Quadrante feito por meio de "login" e "senha" é rastreável, o que permitirá a preservação da segurança das informações confidenciais, pois o colaborador poderá ser identificado individualmente quando utilizar a ferramenta.

A área técnica é responsável pelo rastreamento de acesso às informações confidenciais, especialmente em caso de ameaça ou violação da segurança.

**6.6.4. Acesso ao sistema em caso de mudança de atividade**

A fim de exercer sua função dentro do elevado padrão de qualidade imposto pela Quadrante Investimentos, a mudança de atividade dentre das áreas da Quadrante implica em assumir novas responsabilidades e compromissos.

Dessa forma, o acesso à novas funcionalidades do sistema permitirá que o colaborador transite em um ambiente que antes era restrito a um grupo limitado de pessoas.

Sendo assim, do mesmo modo que já ocorria na ocupação anterior, diante da autorização para acessar informações consideradas confidenciais, deverá o colaborador preservar a confidencialidade de informação relativa a clientes e a empresa.

### 6.6.5. Acesso ao sistema em caso de afastamento ou desligamento de colaborador

Havendo afastamento do colaborador ou o seu desligamento da empresa, todo o seu acesso a dados e informações do sistema serão bloqueados ou cancelados, comunicando-se área de Tecnologia da Informação.

### 6.7. Procedimentos para backup e redundância de informações

Todo ambiente de Tecnologia da Informação que suporta os arquivos digitais da Quadrante Investimentos possui procedimentos de backup, nos quais todas as informações são replicadas. Isso ocorre de duas formas: através de backup físico, utilizando um "hard-disk" específico para armazenamento de arquivos replicados, e em tempo real, através do "armazenamento em nuvem".

## 7. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

Com a finalidade de garantir a integridade, confiabilidade e disponibilidade das informações é importante disseminar a cultura de segurança cibernética.

### 7.1. *Risk Assessment*

Tendo como referência o Guia de Cibersegurança da Anbima, a Quadrante Investimentos busca mapear o risco cibernético, identificando as vulnerabilidades internas e externas a que está exposta.

### 7.2. Medidas de prevenção e proteção

Inúmeras medidas poderão ser utilizadas para impedir um ataque cibernético:

a) Controle de acesso;

b) Estabelecer regras mínimas quando da definição de senhas de acesso;

c) Possibilidade de rastreabilidade e auditoria de eventos utilizando login e alteração de senhas;

d) Permitir a acesso externo e o controle das informações por meio de dispositivos remotos;

e) Permitir somente a utilização de computadores autorizados e software licenciados;

f) Restrição de acesso a área com informações sensíveis ou críticas;

g) Implementar serviço de backup replicando todas as informações que circulam pelo ambiente virtual da empresa;

h) Proibir que seja instalado nos computadores da Quadrante, por colaboradores ou terceiros, qualquer software sem a autorização do diretor responsável pela área de TI.

i) A instalação de qualquer software será realizada somente pela empresa contratada responsável pela tecnologia da informação; e,

j) Instalação de antivírus e firewalls pessoais em estações e servidores de rede.

**7.3. Monitoramento**

O constante monitoramento de acesso às informações permite a identificação de possíveis ameaças ao ambiente tecnológico da Quadrante Investimentos.

Este monitoramento poderá ocorrer de diversas maneiras, dentre elas:

a) Possibilitar a identificação do colaborador e visitante que acessar os dados contidos na rede interna, seja nas dependências da empresa ou remotamente;

b) Realizar testes periódicos de invasão externa e phishing, a fim de analisar as vulnerabilidades da estrutura tecnológica;

c) Realizar inspeção física, a qualquer tempo, nos computadores da Quadrante Investimentos, respeitando a confidencialidade das informações;

d) Registrar continuamente as operações; e,

e) Conduzir investigações internos no tempo e prazo apropriados.

**7.4. Plano de resposta a incidente**

Em caso de qualquer suspeita de violação à integridade de seu sistema computacional, todos os colaboradores da Quadrante Investimentos tem a obrigação de comunicar o fato imediatamente à Diretoria de Controles Internos e Compliance a fim de que sejam tomadas as medidas necessárias pela área de tecnologia da informação que elaborará um plano de ação em conjunto com os demais setores da empresa.

Dentre outros itens, o plano de ação deverá estabelecer as pessoas responsáveis e a sua função a ser exercida durante o evento, bem como a forma com que se será implementado o plano de continuidade de negócios, considerando as ações previstas na respectiva Política de Continuidade de Negócios.

**7.5. Reciclagem**

A constante atualização dos colaboradores se faz necessária a fim de que sejam capazes de identificar novos riscos relacionados à segurança cibernética.

Da mesma forma, as modificações legislativas como a recente Lei nº 13.709/18 denominada Lei Geral de Proteção de Dados, impõe a necessidade de promover a cultura de segurança por meio de treinamentos e divulgação de comunicações relacionadas ao tema.

O auxílio de materiais educativos permitirá conhecer o conteúdo desta Política, assim como seus direitos e deveres acerca do tema “segurança da informação”.

## 8. TREINAMENTO

Todos os colaboradores que já figuram nos quadros da Quadrante Investimentos, assim como aqueles que ingressarem posteriormente deverão receber treinamentos periódicos de capacitação visando a presença, detecção e resposta a incidentes de segurança da informação.

O treinamento poderá ser realizado anualmente, quando da admissão de novo colaborador ou, a qualquer tempo em razão do surgimento de fato relevante.

## 9. TESTES PERIÓDICOS DE SEGURANÇA

Caberá a área de Tecnologia da Informação com o auxílio da área de Controles Internos e Compliance realizar testes e verificações periódicas, a fim de avaliar a integridade e a segurança do sistema e equipamentos.

## 10. PERIODICIDADE DE REVISÃO

Esta Política deverá ser revisada anualmente ou, extraordinariamente, a qualquer tempo em caso de eventuais alterações legais, normativas ou estatutárias.

A revisão da Política de Segurança da Informação será submetida aos membros do Conselho de Administração, para deliberação e aprovação.

A presente Política entrará em vigor na data de sua aprovação.

## 11. CONTROLE DE VERSÕES

| Histórico | Data | Aprovado por: |
|---|---|---|
| **Versão 5** | **2020** | **Conselho de Administração** |
| **Versão 4** | **2019** | **Conselho de Administração** |
| **Versão 3** | **2018** | **Diretoria** |
| **Versão 2** | **2017** | **Diretoria** |
| **Versão 1** | **2016** | **Diretoria** |