POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

JUNHO 2020

MENSAGEM DA REAG DTVM AOS COLABORADORES:

Esta Política de Segurança da Informação ("Política") da REAG DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS S.A. ("REAG DTVM") tem o objetivo de detalhar as práticas e o tratamento adequado às informações produzidas e recepcionadas pela Reag DTVM e acordar com todos os colaboradores os seguintes compromissos:

- Nossos colaboradores mantêm reserva sobre os negócios da Reag DTVM, guardando sigilo sobre qualquer informação ainda não divulgada para o conhecimento do mercado, bem como sobre a informação de terceiros e clientes obtidos no exercício de suas funções;

- Nossos colaboradores não utilizam estas informações para obter, pessoalmente ou para terceiros, vantagens sobre qualquer natureza; e

- A informação é um ativo essencial dos Processos de Negócios da Reag DTVM. Informações reservadas ou confidenciais somente são divulgadas com autorização da Diretoria. Todo colaborador que possui acesso a estas informações tem o cuidado de não as expor a terceiros.

O envolvimento e a adesão consciente de cada um dos colaboradores a essa Política serão fundamentais para consolidarmos o comportamento coletivo cada vez mais atento e seguro quanto ao tratamento das informações internas.

Este documento apresenta as Normas Gerais para uso adequado das informações e recursos de tecnologia na Reag DTVM e orientará nossas atitudes sobre o tema, oferecendo padrões de comportamento a serem seguidos.

Atenciosamente,

Reag DTVM

1. OBJETIVO:

O objetivo desta norma é definir as regras para o uso adequado das informações e dos recursos de tecnologia da informação da Reag DTVM.

2. ABRANGÊNCIA:

Esta Política aplica-se a todos os sócios, administradores e funcionários da Reag DTVM, ("Colaboradores" ou, quando referido individual e indistintamente, "Colaborador").

3. PRINCÍPIOS:

A Reag DTVM tem o compromisso com o tratamento adequado das informações da empresa, e de seus clientes está fundamentado nos seguintes princípios:

- Confidencialidade: o acesso à informação é garantido somente a pessoas autorizadas e quando ele for de fato necessário;
- Disponibilidade: que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- Integridade: a exatidão e a completude da informação e dos métodos de seu processamento são garantidas pela Reag DTVM, bem como a transparência no trato com os clientes e Colaboradores.

4. RESPONSABILIDADES:

4.1. COMPLIANCE:

- Manter atualizada a Política;
- Elaborar, manter atualizado e testar periodicamente um Plano de Contingência; e,
- Tratar dúvidas e questões não contempladas pela Política de Segurança da Informação;

4.2. GESTORES DAS ÁREAS:

- Garantir a aplicação adequada da Política, apoiados pela Diretoria da Reag DTVM.

4.3. COLABORADORES E DEMAIS ENVOLVIDOS

- Utilizar adequadamente as informações e os recursos computacionais oferecidos, em conformidade com os objetivos do negócio e as normas expressas nesta política e no Manual de Compliance.

5. CRITÉRIOS E REGRAS:

5.1. PROPRIEDADE E PROTEÇÃO DA INFORMAÇÃO:

- Toda a informação produzida pela Reag DTVM, é considerada de sua propriedade, sendo parte do seu patrimônio, não importando a forma de apresentação ou armazenamento. Esta informação deve ser adequadamente protegida e utilizada apenas no interesse da Reag DTVM. Seu uso ou divulgação externa somente poderá ocorrer quando expressamente autorizado pela diretoria da empresa;
- Tecnologias, marcas, metodologias e quaisquer informações que pertençam a Reag DTVM não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.
- As informações e documentos disponibilizados pelos clientes da Reag DTVM serão adequadamente protegidos e armazenados, observado a legislação e regulamentação pertinentes. Seu uso ou divulgação externa somente poderá ocorrer quando expressamente autorizado pela diretoria da empresa; e
- A Reag DTVM poderá monitorar o recebimento, envio e conteúdo de todos os e-mails, arquivos e documentos de sua propriedade sem prévia notificação aos usuários.

5.2. DIVULGAÇÃO

- A Reag DTVM disponibilizará uma cópia desta Política para consulta, em sua respectiva sede, e no ato da admissão de cada um de seus novos Colaboradores.

5.3. CONTRATOS DE SERVIÇOS (TERCEIROS)

- Nos contratos de prestação de serviços deve haver cláusula específica expondo a obrigatoriedade do cumprimento da Política pelo fornecedor contratado pela Reag DTVM, para o qual deverá ser disponibilizada uma cópia desta Política.

6. CLASSIFICAÇÃO DA INFORMAÇÃO:

- Informações estratégicas da Reag DTVM, enquanto não divulgadas de forma oficial, são consideradas estritamente confidenciais;
- Informações dos clientes da Reag DTVM e das operações por eles solicitadas são consideradas sigilosas, conforme legislação e regulamentação pertinentes;
- O Colaborador da Reag DTVM é responsável por garantir a segurança da informação sob a sua guarda; e
- Não é permitido divulgar informações confidenciais, seja através de conversas informais, e-mails ou qualquer outro meio de comunicação, sem a prévia autorização.

7. SEGURANÇA FÍSICA E DO AMBIENTE:

7.1. ACESSO FÍSICO

- O acesso físico ao ambiente de TI somente será permitido por pessoas autorizadas pelo Diretor de Compliance.
- Para acesso às dependências em horários alternativos (finais de semana, feriados, etc.) será necessária a aprovação da Diretoria; e
- O acesso às dependências da Reag DTVM em horários alternativos exceto diretoria, gerência, e coordenadores deverá ser previamente informado ao Departamento de TI, pelo responsável pela área.

7.2. ZELO COM AS INFORMAÇÕES

- A informações classificadas como sigilosas, confidenciais e/ou estratégicas não devem ser deixadas sobre a mesa de trabalho, devendo ser armazenados dentro de gavetas ou armários;
- As informações confidenciais devem ser totalmente destruídas quando não mais necessárias, independentemente do tipo de mídia em que estiverem armazenadas;
- As impressões no ambiente de trabalho serão controladas por senha individual. Os arquivos que permanecerem na fila de impressões serão ao final do expediente descartados;
- O Colaborador deve sempre bloquear sua estação de trabalho quando interromper o uso, mesmo que por breve momento; e
- O armazenamento de arquivos de dados da Reag DTVM e de seus clientes não pode ser salvo no disco local dos computadores, devendo ser utilizados os drives da rede para tal, onde dispositivos de segurança asseguram o correto tratamento desta informação.

7.3. COMPUTAÇÃO MÓVEL/COMPUTAÇÃO DE TERCEIROS

- O acesso a computação móvel será permitido somente à Diretoria, exceções devem ser autorizadas previamente pela Diretoria;
- Quando solicitado algum equipamento, o usuário preencherá um termo de responsabilidade disponibilizado pelo Departamento de TI. O usuário irá zelar pelo equipamento sob sua guarda, devendo utilizá-lo e movimentá-lo atendendo exclusivamente aos interesses da Reag DTVM;
- Não é permitido o uso de equipamentos pessoais, sistemas ou arquivos nas dependências da empresa ou no desenvolvimento das funções do Colaborador, salvo em exceções autorizadas pela Diretoria;
- Os prestadores de serviços terceirizados alocados na empresa deverão utilizar equipamentos fornecidos pela própria Reag DTVM; e,
- Caso os prestadores de serviços utilizem equipamentos próprios, estes somente terão acesso à rede *wireless guest*, desde que seu equipamento atenda aos requisitos mínimos de segurança previstos nesta Política.

8. OPERAÇÃO DO AMBIENTE COMPUTACIONAL:

8.1. OPERAÇÃO DOS RECURSOS DE PROCESSAMENTO DAS INFORMAÇÕES

8.1.1 Conexões de Rede

- Equipamentos conectados à rede wireless devem ter antivírus com a data da última atualização não superior a três dias;
- A Reag DTVM poderá acessar e auditar os equipamentos dos colaboradores e prestadores de serviços para garantir a segurança geral de seu ambiente computacional sem prévio aviso;
- É proibido utilizar conexão discada via modem, ADSL ou quaisquer outras formas, nos equipamentos que estejam, ao mesmo tempo, conectados na rede local da Reag DTVM.

8.1.2 Senhas

- A senha é pessoal e intransferível, devendo obedecer aos padrões divulgados pela empresa. O Colaborador é responsável por todas as transações realizadas nos sistemas disponibilizados;
- A senha não deve, sob hipótese alguma, ser compartilhada com outras pessoas;
- O usuário não deve armazenar sua senha em arquivos de computador e tampouco escrevê-la em papéis ou outro tipo de mídia;
- As senhas de logon na rede devem estar de acordo com os seguintes aspectos:
  a) Conter no mínimo 6 (seis) caracteres;
  b) Possuir letras e números; e
  c) Devem ser criptografadas quando transmitidas ou armazenadas.
- As senhas do Protheus 10 devem estar de acordo com os seguintes aspectos:
  d) Conter no mínimo 6 (quatro) caracteres; e
  e) Devem ser criptografadas quando transmitidas ou armazenadas.
- As senhas de logon e do Protheus terão validade de no máximo 90 (noventa) dias; e
- Critérios de senhas de outros sistemas de trabalho das áreas devem ser decididos pela Diretoria.

8.1.3 Hardware e Software

- Não é permitida a instalação e utilização de unidades de armazenamentos removíveis (pen drives, HDs externos, cartão de memória, mp3 e outros), salvo em casos autorizados pela Diretoria;
- Não é permitida a compra de equipamentos de tecnologia e softwares sem a prévia comunicação e aprovação da Diretoria;

8.1.4 Alterações de Configuração

- As configurações de hardware e software dos computadores disponibilizados pela Reag DTVM não devem ser alteradas. Caso haja necessidade de algum tipo de alteração, a Diretoria deverá ser acionada através de solicitação por e-mail.

8.1.5 Internet

- A Internet é uma ferramenta de trabalho utilizada pelos Colaboradores como apoio ao desenvolvimento de suas atividades e competências; e
- Não é permitido o acesso a e-mails pessoais e software de comunicação entre outros, caso necessário o Colaborador deverá solicitada autorização ao seu gestor responsável, que requererá a aprovação da Diretoria.

8.2. PROTEÇÃO CONTRA SOFTWARE MALICIOSO

- O software de proteção contra vírus deve ser instalado, ativado e atualizado diariamente em todos os computadores ligados à rede de dados da Reag DTVM; e
- Os softwares deverão ser devidamente atualizados conforme recomendação dos seus fabricantes e/ou desenvolvedores.

8.3. CÓPIA DE SEGURANÇA (*BACKUP*)

- Cabe ao Departamento de TI realizar regularmente a cópia dos dados e informações mantidas nos equipamentos de armazenamento nos servidores da empresa;
- Backup de e-mails armazenados nos computadores locais e móveis ingressados no domínio Reag DTVM será realizado mensalmente; e

- A pedido da Diretoria, o Departamento de Facilities - TI poderá realizar cópias extraordinárias dos dados e informações mantidos e armazenados nos equipamentos, servidores da empresa e dos e-mails dos Colaboradores, sem prejuízo das cópias de segurança realizadas na periodicidade indicada acima.

8.4. TRATAMENTO DE MÍDIA

- Não é permitido realizar cópia ou divulgar informações confidenciais e sigilosa para uso pessoal ou de terceiros. Tais cópias ou divulgações, quando necessárias, devem ser autorizadas previamente pela Diretoria.

8.5. TRATAMENTO DE MÍDIA

- Não é permitido realizar cópia ou divulgar informações confidenciais e sigilosa para uso pessoal ou de terceiros. Tais cópias ou divulgações, quando necessárias, devem ser autorizadas previamente pela Diretoria.

8.6. TROCA DE INFORMAÇÕES

- **Uso do Correio Eletrônico (e-mail)**

- A autorização de acesso ao correio eletrônico deve ser solicitada ao Departamento de TI, que tomará as providências necessárias para tanto;
- O Correio Eletrônico é uma ferramenta de trabalho utilizada pelos Colaboradores, como apoio ao desenvolvimento de suas atividades profissionais;
- Não é permitido utilizar o Correio Eletrônico para o envio de mensagens ou arquivos de conteúdo considerado impróprio pela empresa;
- É considerado impróprio o conteúdo que não está em conformidade com as regras legais, a moral, a integridade e os bons costumes, tais como campanhas políticas, religiosas, venda de produtos, boatos, jogos, músicas, filmes, vídeos e fotos que não esteja na conformidade do negócio;
- O endereço oficial da empresa, assim como as caixas postais a eles associadas são de propriedade da Reag DTVM;

- É proibido o download e envio de arquivos anexados ao e-mail com as extensões *.exe, *.pif, *.bat, *.com, *.scr, *.mp3, *.wav, *.wma, *.vbs, *.reg;

- Todos os e-mails do domínio, exceto os de gerentes e diretores, serão armazenados pelo Departamento de TI, para auditorias internas e externas, e poderão ser consultados com a autorização da diretoria a qualquer momento sem prévio aviso; e

- Práticas recomendadas na utilização o e-mail:

a) Envie e-mails apenas para os destinatários que realmente precisam da informação;
b) Seja breve, pois assim, dificilmente as pessoas deixarão de ler a sua mensagem;
c) Sempre que possível, não utilize anexos no e-mail; e
d) Seja educado, não escreva nada que não diria pessoalmente.

- **Uso de Criptografia**

- Somente é permitida a utilização de mecanismos de criptografia homologados pela Reag DTVM. Em caso de necessidades adicionais, o Departamento de TI deverá ser acionada através de solicitação da área administrativa.

8.7. SOFTWARES E RECURSOS DE INFORMÁTICA

- **Instalação de Softwares**

- Somente é permitida a utilização de software devidamente homologado, licenciado, instalado e controlado pelo Departamento de TI; e

- Os softwares serão devidamente atualizados de acordo com as recomendações de seus fabricantes e/ou desenvolvedores.

- **Instalação e movimentação de Recursos de Informática**

- A instalação, controle, movimentação e manutenção de recursos computacionais de propriedade da Reag DTVM são de responsabilidade exclusiva do Departamento de TI.

9. CONTROLE DE ACESSO:

9.1. ACESSO LÓGICO

- Cada usuário de recursos computacionais da Reag DTVM deve possuir uma identificação (ID), a qual será utilizada como "conta de acesso" aos sistemas e redes da empresa determinadas a sua área;
- O cadastramento do usuário para o acesso aos recursos computacionais deve ser solicitado pela área administrativa ao Departamento de TI, o qual estabelecerá os perfis e autorizações de acesso;
- O usuário deve ter acesso somente às informações e recursos que forem necessários para a realização de suas atividades;
- As movimentações de pessoal (admissões, transferências, promoções, demissões, etc.) devem ser comunicadas pela área administrativa ao Departamento de TI, a fim de que as devidas atualizações nos ambientes computacionais sejam realizadas;
- Cabe ao gestor responsável por cada um dos contratos com fornecedores, quando do encerramento dos mesmos, solicitar por escrito à área administrativa o cancelamento dos acessos concedidos.

9.2. DESLIGAMENTOS

- Será de responsabilidade da área administrativa informar os desligamentos de Colaboradores imediatamente para o Departamento de TI, o qual realizará os bloqueios de acesso de imediato;
- O Colaborador deverá entregar todos os equipamentos de sua responsabilidade para o Departamento de TI no momento de seu desligamento, como, por exemplo: celulares, notebooks, pen drives e outros, sob pena de restituição dos valores relativos a cada um dos equipamentos.
- Dados de usuários desligados da Reag DTVM serão armazenados para utilização exclusiva da Reag DTVM e o e-mail redirecionado para o gestor da área. O Colaborador desligado não poderá realizar cópia de arquivos para sua utilização fora da empresa.

10. PLANO DE CONTINGÊNCIA:

Cabe ao Departamento de TI manter atualizado e testar periodicamente o Plano de Contingência que garanta a continuidade das atividades críticas aos negócios da Reag DTVM.

11. CONFORMIDADE:

A Reag DTVM, seus Colaboradores e todos aqueles que estejam envolvidos com suas atividades devem estar em conformidade com essa Política.

12. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

Violações a essa Política estão sujeitas a sanções disciplinares, observadas a natureza e gravidade da infração, e na legislação vigente no Brasil.

Ao identificar ou suspeitar de possível violação das diretrizes estabelecidas nessa Política informar ao Departamento de Compliance.

Em caso de dúvida sobre essa Política de Segurança da Informação entre em contato com o Departamento de Compliance: *compliance@reagdtvm.com.br*.

Qualquer outra informação, o Colaborador deve buscar orientação junto ao seu gestor imediato e ao Diretor de Operações.