Política de Segurança da Informação
Bahia AM Renda Variável Ltda. e Bahia AM Renda Fixa Ltda.

01. OBJETIVO: 3
02. CONCEITUAÇÃO / DEFINIÇÃO: 3
03. ABRANGÊNCIA: 3
04. RESPONSABILIDADES: 3
04.01. Responsáveis pela execução das atribuições da Política: 3
04.01.01. Usuários: 3
04.01.02. Gestores de Informações: 4
04.01.03. Administradores dos Ativos de TI: 4
04.02. Responsáveis pelo monitoramento da execução das atribuições da Política: 4
04.03. Responsáveis pela manutenção da Política: 4
05. DIRETRIZES: 4
05.01. Acesso a Informações: 4
05.02. Ambiente de TI 5
05.03. Propriedade dos dados 5
05.04. Chaves de Acesso: 5
05.04.01. Senhas Orientações Gerais 5
05.04.02. Sistema Operacional e Sistemas desenvolvidos internamente 6
05.04.03. Sistemas desenvolvidos externamente e sistemas externos 6
05.05. Contingência 6
05.06. Backup 7
05.06.01. Frequências de Backup 7
05.06.02. Descarte de Informação 7
05.06.03. Testes 7
05.06.04. Recuperação de Dados 7
05.07. E-mail 7
05.07.01. Autenticação no serviço de e-mail 7
05.07.02. Uso do serviço de e-mail dentro da rede interna 7
05.07.03. Uso do serviço de e-mail fora da rede interna 7
05.07.04. Política de segurança de acesso à e-mail em dispositivos móveis 8
05.08. Acesso Remoto 9
05.09. Uso de Ferramentas de Inteligência Artificial 9
05.010. Registro de atividades 9
05.011. Sanções disciplinares 9

06. ALÇADAS: 10
07. CONSIDERAÇÕES FINAIS: 10
08. LEGISLAÇÃO / REGULAÇÃO RELACIONADA: 10
09. REFERÊNCIA INTERNA: 10
010. BIBLIOGRAFIA: 10
011. GLOSSÁRIO: 10

01. OBJETIVO:

A Bahia AM Renda Variável Ltda. e a Bahia AM Renda Fixa Ltda. (doravante denominadas em conjunto "Gestoras") visam estabelecer padrões de comportamento com relação ao manuseio de informações para minimizar a ocorrência de incidentes de segurança e preservar a confidencialidade, a integridade e a disponibilidade delas, bem como a devida segregação, quando aplicável, conforme definido na regulação.

02. CONCEITUAÇÃO / DEFINIÇÃO:

A informação é um ativo que tem alto valor para as Gestoras, tendo isso em vista, toda informação/sistema possui um responsável pela definição da sua segurança de acesso, conforme listado no anexo I.

A Segurança da Informação refere-se à proteção da informação e é orientada pelos conceitos de confidencialidade, integridade e disponibilidade.

03. ABRANGÊNCIA:

A presente Política aplica-se a todos os sócios, administradores, empregados, estagiários (doravante denominada em conjunto "Colaboradores") das Gestoras, inclusive prestadores de serviços (todos em conjunto designados "usuários" ou individualmente "usuário") que tiverem acesso às informações desenvolvidas, de propriedade das Gestoras ou relativas às suas atividades através de recursos de Tecnologia da Informação ("TI") ou por qualquer outro meio de processamento, comunicação ou armazenamento.

Ao ingressarem nas Gestoras todos os colaboradores foram devidamente apresentados às Políticas Internas e aderiram às mesmas atestando, dessa forma, seu conhecimento acerca das normas estabelecidas e comprometendo-se a observá-las no exercício de suas respectivas atividades restando, assim, cientes que os ambientes, sistemas, computadores e redes das Gestoras poderão ser monitorados, auditados e gravados.

04. RESPONSABILIDADES:

04.01. Responsáveis pela execução das atribuições da Política:

04.01.01. Usuários:

É de responsabilidade de todos os colaboradores:

- Zelar pela segurança das informações e equipamentos das Gestoras utilizando-os, sempre, de forma compatível com esta Política, legislação e regulação aplicáveis;
- Respeitar os controles de segurança implantados no ambiente de TI com o objetivo de reforçar o cumprimento desta Política;
- Estar ciente de que somente os dados armazenados em servidores da rede corporativa estão sujeitos aos procedimentos de backup e contingência, sendo assim, os dados armazenados de forma diferente não possuem garantia de disponibilidade. Por tal motivo, os dados não devem ser armazenados localmente nos desktops ou nos dispositivos móveis, ademais, os desktops podem ter seus dados apagados pela TI a qualquer momento por questões de segurança;
- Não armazenar ou manusear dados pertencentes às Gestoras em equipamentos particulares ou de terceiros, salvo equipamentos homologados e disponibilizados pela TI; e
- Informar ao Compliance caso verifique o descumprimento de alguma norma ou diretriz ou, ainda, se algum controle estiver ausente ou sendo burlado. Em adição, são exemplos de

violações de acesso o recebimento de correios eletrônicos e acesso a páginas web em desacordo com a legislação e regulação em vigor.

04.01.02. Gestores de Informações:

Os Gerentes e Diretores são os gestores da informação vinculada às áreas sob sua responsabilidade, portanto, é responsabilidade dos gestores das informações:

- Zelar pela segurança das informações geridas definindo, com isso, os requisitos de confidencialidade, integridade e disponibilidade das mesmas;
- Aprovar os controles de segurança para as informações geridas;
- Autorizar e revogar permissões de acesso às informações geridas mantendo, assim, o controle das listas de acesso;
- Ao autorizar um acesso, informar o usuário do nível de criticidade e da forma de utilização das informações em questão.

04.01.03. Administradores dos Ativos de TI:

Os profissionais da equipe de TI, respeitada a hierarquia, são os administradores dos Ativos de TI e, portanto, responsáveis por:

- Zelar pela segurança das informações e equipamentos disponibilizados pelas Gestoras garantindo, assim, que eles estejam configurados de acordo com as melhores práticas de segurança, as normas e os procedimentos de configuração internos;
- Garantir que os usuários tenham os privilégios mínimos nos dispositivos sob sua administração para que seja possível a realização de suas atividades;
- Orientar os demais usuários quanto às melhores práticas e à presente Política;
- Implementar controles de acesso às informações e demais ativos de TI de acordo com o determinado pelos gestores das informações sob sua administração.

04.02. Responsáveis pelo monitoramento da execução das atribuições da Política:

É responsabilidade da área de TI assegurar a execução da presente Política e monitorar as atividades dos usuários e fornecedores para assegurar a execução desta Política.

04.03. Responsáveis pela manutenção da Política:

É responsabilidade das áreas de TI a manutenção e atualização desta Política.

05. DIRETRIZES:

05.01. Acesso a Informações:

- O usuário deve ter acesso somente às informações necessárias para o desempenho de suas atividades determinadas pelas Gestoras;
- O usuário é responsável por todas as ações realizadas através de suas chaves de acesso, as quais são pessoais, intransferíveis e de responsabilidade do usuário. Tendo isso em vista, entende-se por chave de acesso qualquer forma de identificação que permita acesso a alguma informação das Gestoras;
- Somente é permitida a saída de informações das dependências das Gestoras ou o compartilhamento no âmbito das Gestoras se contemplada pelos critérios estabelecidos por política ou procedimento relacionado ao assunto. A referida saída deve pautar-se sempre no conceito de que o receptor deve ser alguém que necessita receber tais informações para o

desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação.

- Todos os arquivos em trânsito devem ser criptografados. Em caso de dúvidas, a área de TI deverá ser acionada previamente à revelação.
- Para obedecer às regras de segregação de áreas e funções, as Gestoras adotam uma rede de diretórios segmentada bem como perfil específico para cada departamento nos sistemas internos a fim de impedir que arquivos e informações de um determinado departamento sejam indevidamente acessados por outro departamento e, dessa forma, limitar o acesso a informações confidenciais e evitar situações que poderiam gerar conflitos de interesse.

05.02. Ambiente de TI

- Qualquer recurso tecnológico somente pode ser utilizado no ambiente das Gestoras após a homologação e autorização pelo departamento de TI;
- Todos os recursos de TI devem ser protegidos contra acessos indevidos e ter sua documentação atualizada e padronizada;
- Todos os recursos de TI devem estar de acordo com as cláusulas contratuais acordadas com fornecedores e com a legislação vigente; e
- Fornecedores, clientes e convidados poderão ter acesso à rede das Gestoras desde que limitados. Para solicitar acesso a um parceiro externo o colaborador deverá entrar em contato com o departamento de TI.

05.03. Propriedade dos dados

- Todos os dados e informações criados no ambiente das Gestoras, mesmo que para uso individual, são propriedade das Gestoras;
- Todos os dados armazenados nos recursos de TI das Gestoras devem ter um responsável, o qual será denominado gestor e deverá ter um nível hierárquico mínimo de Gerente. Em acordo com o item anterior, a gestão das informações não indica propriedade sobre elas;
- As Gestoras não se responsabilizam pela privacidade, manutenção e guarda de dados pessoais dos Colaboradores armazenados no ambiente das Gestoras por ação dos Colaboradores, uma vez que se veda a utilização da rede corporativa para guarda de dados pessoais dos Colaboradores. Destaca-se que não é autorizada a realização de cópia/disponibilização destes dados no desligamento do colaborador; e
- Qualquer exceção aos itens anteriores no tocante a permissões, deverão ser analisadas conjuntamente pelo gestor conforme acima mencionado, pela área de Compliance e pela área de TI.

05.04. Chaves de Acesso:

05.04.01. Senhas Orientações Gerais

- Não é permitido o compartilhamento de sua(s) chave(s) de acesso e em caso de suspeita da perda de sigilo a(s) chave(s) de acesso deve(m) ser trocada(s) imediatamente;
- A senha do colaborador é pessoal e intransferível logo, não deve ser compartilhada com colegas de trabalho, assistentes, secretárias ou qualquer outra pessoa, mesmo quando o colaborador viajar ou sair de férias. Reitera-se que a senha não deve ser enviada por e-mail a ninguém;
- Deve-se utilizar um método próprio para lembrar as senhas que dispense registrá-las em qualquer local como, por exemplo, podem ser utilizados acrônimos, ou seja, palavras formadas pelas letras ou sílabas iniciais de palavras de uma frase;

- Não devem ser utilizadas senhas com informações pessoais fáceis de serem obtidas, tais como: nome ou sobrenome do usuário, nome do cônjuge, filhos, animais de estimação, número de telefone, data de nascimento, cidade de origem, entre outros;
- É desejável que as senhas utilizadas possam ser digitadas rapidamente, sem que seja preciso olhar para o teclado;
- Não é recomendado o uso de palavras existentes em dicionários nacionais ou estrangeiros;
- Não devem ser utilizadas senhas com números ou letras repetidas em sequência;
- Não devem ser utilizadas sequências numéricas, alfabéticas ou do teclado; e
- Quanto a chaves de acesso em meio tecnológico o colaborador deverá seguir as orientações descritas na Política de Utilização dos Recursos de TI.

05.04.02. Sistema Operacional e Sistemas desenvolvidos internamente

As senhas de rede de todos os usuários terão validade de quarenta e dois dias. Ao final deste período será pedido, no momento do login, que o usuário cadastre novamente sua senha. As senhas deverão ter pelo menos sete caracteres e conter pelo menos três entre os seguintes tipos de caracteres:

- Maiúsculos do inglês (A-Z);
- Minúsculos do inglês (a-z);
- Numéricos (0-9); e
- Não-alfanuméricos (!, @, #, $, %, &, entre outros).

Exemplo: A partir da frase “Brasil campeão na África do Sul” cria-se uma senha com o acrônimo Bc10nAdS, no qual B, c e 1 atendem ao requisito de três tipos diferentes de caracteres.

Ademias, senhas utilizando caracteres acentuados devem ser evitadas e usuários de acesso remoto só devem utilizar caracteres maiúsculos e minúsculos (com até três tentativas inválidas).

O usuário poderá efetuar até seis tentativas inválidas até que a sua senha seja bloqueada. As últimas dez senhas utilizadas pelo usuário ficarão registradas e o usuário não poderá repeti-las. Se o padrão de senhas aqui definido for modificado, a área de TI avisará aos masters dos sistemas para que eles promovam a adequação das senhas ao novo padrão.

Os sistemas internos seguirão o padrão de senhas definido nesta Política. Qualquer exceção deverá ser comunicada e aprovada pela área de Compliance.

05.04.03. Sistemas desenvolvidos externamente e sistemas externos

As senhas utilizadas em sistemas desenvolvidos externamente ou em sistemas externos deverão se adaptar, sempre que possível, ao padrão definido para as senhas de sistemas desenvolvidos internamente.

Quando possível, deverão ser efetuadas configurações nos sistemas que permitam o enquadramento das senhas ao padrão mencionado ou, ainda, deverão ser solicitadas customizações ao fornecedor do sistema.

Para os sistemas nos quais não seja possível utilizar senhas que se enquadrem no padrão definido deve ser informada a área de TI.

05.05. Contingência

As informações e processos dos quais depende a continuidade dos negócios das Gestoras deverão contar com planos de contingência em ambiente de produção e cópias de segurança.

05.06. Backup

As cópias de segurança das informações dos servidores de produção são armazenadas em nuvem, que segue as melhores práticas de mercado para garantir a segurança e confiabilidade das informações.

05.06.01. Frequências de Backup

- **Backup Diário** – é realizado um backup completo, no qual é guardada uma cópia dos arquivos criados ou alterados desde o último backup diário, sendo que essa frequência de backup é retida por sessenta dias em nuvem;
- **Backup Mensal** – é realizado um backup completo de todos os servidores, sendo que essa frequência de backup é retida por cinco anos em nuvem.

05.06.02. Descarte de Informação

As informações dos backups diários e mensais, feitos em nuvem, são sobrescritas após o período de retenção descrito acima.

05.06.03. Testes

São realizados testes mensais, nos quais são recuperados arquivos aleatórios a fim de comprovar a eficiência do processo de backup. Os resultados desses testes serão analisados e armazenados pela área TI.

05.06.04. Recuperação de Dados

Informações do backup diário de até dois dias a partir da data de solicitação serão recuperadas imediatamente pelo usuário, contudo, as informações do backup diário superiores a dois dias e as informações do backup mensal devem ser solicitadas para a TI. O acesso às informações recuperadas deve seguir as diretrizes de acesso à informação desta Política.

05.07. E-mail

Como solução de e-mail utilizamos a plataforma Office 365 da Microsoft em nuvem.

05.07.01. Autenticação no serviço de e-mail

O acesso no serviço de e-mail deve considerar múltiplos fatores de autenticação. Além de usuário e senha, será exigida a utilização do aplicativo *Microsoft Authenticator* ou envio de SMS.

Para as caixas de e-mail associadas a um usuário de rede a senha será sincronizada com a senha de rede.

Para as caixas de e-mail que não estiverem associadas a um usuário de rede a gestão da senha deverá ser realizada pelo gerente da área responsável pela caixa de e-mail.

05.07.02. Uso do serviço de e-mail dentro da rede interna

O acesso ao serviço de e-mail dentro da rede interna pode ser feito por *Outlook* ou *webmail*.

05.07.03. Uso do serviço de e-mail fora da rede interna

A questão envolvendo o trabalho remoto tomou contornos na atualidade, motivo pelo qual torna-se ainda mais necessário a definição clara sobre as regras envolvendo o uso de equipamentos de forma remota pelos Colaboradores das Gestoras.

Entende-se por dispositivos móveis os equipamentos ou mídias digitais que possam acessar o ambiente de rede corporativa da empresa e sejam facilmente transportados por seus utilizadores, tais como notebooks, tablets, smartphones e tokens.

O acesso aos e-mails na rede externa será feito exclusivamente através de dispositivos móveis (Celular e Tablet) que se adequem à Política de segurança das Gestoras, em atendimento à confidencialidade legal e regulatória exigidas, ainda que os dispositivos sejam de propriedade pessoal do usuário.

Os usuários que desejarem utilizar a ferramenta webmail o acesso aprovado pelo diretor da área solicitante e pelo diretor responsável pela segurança da informação.

Para os usuários que sejam Colaboradores sujeitos a registro da jornada de trabalho o acesso ao serviço de e-mail fora dos horários de trabalho trata-se de mera conveniência posta à disposição daqueles, portanto, não é obrigatório o acesso ou resposta pelos Colaboradores.

05.07.04. Política de segurança de acesso à e-mail em dispositivos móveis

Os usuários que optarem pelo uso do serviço de e-mail através de aplicativos em dispositivos móveis, sejam eles corporativos ou próprios, deverão instalar o aplicativo Microsoft Intune (Portal da Empresa) e aceitar a aplicação da Política de Segurança nesses equipamentos.

A Política será aplicada de forma automática no dispositivo móvel durante a configuração do aplicativo Microsoft Intune (Portal da Empresa) e impõe as seguintes configurações:

- Criptografia de dados: o dispositivo será configurado para criptografar os dados;
- Senha: o dispositivo será configurado para exigir uma senha de no mínimo 4 (quatro) caracteres;
- Bloqueio de tela por inatividade: o dispositivo será configurado para bloquear a tela após 1 (um) minuto de inatividade;
- Apagar os dados em caso de falhas na autenticação: o dispositivo será configurado para apagar os dados após 10 (dez) tentativas erradas de autenticação; e
- Apagar os dados em caso de perda ou roubo: o dispositivo será configurado para permitir a que a TI apague todos os dados remotamente.

Além disso, o Colaborador deverá:

- Instalar somente os softwares e as atualizações de software que são disponibilizados pelo departamento de TI;
- Manter o dispositivo atualizado instalando as atualizações e patches de softwares quando eles estiverem disponíveis;
- Manter atualizadas as informações de garantia relevantes para seu dispositivo;
- Informar imediatamente, em um prazo máximo de 24 (vinte e quatro) horas, caso um dispositivo seja perdido, roubado ou comprometido a TI e seu superior hierárquico;
- Certificar-se sempre que possível de que o dispositivo esteja protegido por senha;
- Executar sempre cópias de segurança de todos os dados, configurações, mídias e aplicativos;
- Manter dados pessoais e informações sensíveis em formato criptografado sempre que possível;
- Não clicar ou seguir links recebidos por meio de mensagens eletrônicas;

- Configurar sempre que possível os dispositivos para que possam ser localizados e bloqueados remotamente por meio de serviços de geolocalização;
- Apagar remotamente todos os dados nele armazenados quando necessário.

Caso o Colaborador use dispositivo próprio para trabalhar remotamente será sua responsabilidade notificar a operadora de celular (provedora de serviços) caso o dispositivo seja perdido, roubado ou furtado, bem como solicitar o bloqueio do número (chip) e efetuar as demais medidas cabíveis.

O Colaborador é responsável pela segregação segura de dados corporativos e pessoais. Desta forma, as políticas da empresa serão aplicadas apenas aos dados e aplicativos relacionados ao trabalho e a qualquer acesso corporativo à rede.

O Colaborador não deverá trabalhar remotamente fora dos horários, bem como deve abster-se de realizar horas excedentes quando estiver trabalhando remotamente. Ademais, se existir a necessidade de labor extraordinário ou fora dos horários comerciais, o Colaborador deverá solicitar autorização prévia ao superior hierárquico, por qualquer meio eficaz, que poderá, a seu critério, autorizar ou não a realização do trabalho.

Salvo expressa menção nas mensagens trocadas entre colaboradores da empresa em sentido contrário, por exemplo, urgente, etc, em regra o Colaborador deve se abster de responder mensagens fora da sua jornada de trabalho.

05.08. Acesso Remoto

O acesso remoto é uma ferramenta que possibilita que todos os Colaboradores com computadores cadastrados possam acessar a rede e realizar suas rotinas de fora do escritório.

O acesso remoto deve ser utilizado para permitir o trabalho remoto (home office) e garantir a continuidade dos processos em casos de incidentes de causas naturais ou no ambiente físico do prédio, nos quais a estrutura de rede permaneça intacta. Para conexão no acesso remoto será exigida a utilização de múltiplos fatores de autenticação e a instalação do aplicativo de VPN.

05.09. Uso de Ferramentas de Inteligência Artificial

A utilização de ferramentas de Inteligência Artificial dentro da empresa é restrita e deve ser realizada de acordo com as diretrizes estabelecidas nesta política. Neste contexto, a única ferramenta aprovada para uso interno é o Bahia ChatGPT. Todos os Colaboradores devem se abster de utilizar outras plataformas ou softwares de Inteligência Artificial que não estejam devidamente autorizados, a fim de garantir a segurança da informação e a proteção dos dados da empresa.

O acesso a ferramenta do Bahia ChatGPT pode ser feito através do link:

- https://bahiachatgpt.azurewebsites.net/

05.010. Registro de atividades

O acesso e uso de qualquer informação ou recurso de TI das Gestoras poderá ser registrado através de trilhas de auditoria.

05.011. Sanções disciplinares

O comportamento em desacordo com a presente Política implicará sanções disciplinares de acordo com os procedimentos internos e a legislação vigente, as quais podem variar de advertência a até o desligamento do Colaborador, de acordo com o que for deliberado pela Diretoria.

06. ALÇADAS:

O Compliance é responsável pela aprovação de situações não previstas nesta Política.

07. CONSIDERAÇÕES FINAIS:

A presente Política cancela qualquer outra forma de divulgação anterior sobre o tema Segurança da Informação.

Quaisquer dúvidas, esclarecimentos ou denúncias deverão ser encaminhados ao Compliance através do e-mail compliance@bahiaasset.com.br .

08. LEGISLAÇÃO / REGULAÇÃO RELACIONADA:
N/A.

09. REFERÊNCIA INTERNA:
N/A.

010. BIBLIOGRAFIA:
N/A.

011. GLOSSÁRIO:
N/A.