POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

CAPÍTULO I - OBJETIVO

A Presente Política de Segurança da Informação e Segurança Cibernética ("**Política**") tem como objetivo precípuo a definição de regras e princípios norteadores das condutas dos colaboradores da R I – Administradora de Carteira de Valores Mobiliários Ltda. ("**RI GESTORA**"), assim entendidos seus (i) sócios; (ii) diretores; (iii) funcionários; (iv) estagiários; ou (v) de quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Sociedade, tenham acesso a informações relevantes sobre a Sociedade, seus negócios ou clientes, em especial no que se refere à segurança da informação e segurança cibernética.

Os colaboradores atestam a ciência e adesão acerca dos procedimentos definidos pela presente Política mediante assinatura de termo próprio, sendo submetidos anualmente ao Programa de Treinamento adotado pela **RI GESTORA**, a fim de que sejam orientados sobre as rotinas a serem observadas no desempenho dos processos descritos nesta Política.

A **RI GESTORA** coletará Termo de Confidencialidade de quaisquer terceiros contratados que tiverem acesso às informações confidenciais a respeito da **RI GESTORA**, seus colaboradores, fundos sob gestão e investidores, salvo se este compromisso já tiver sido firmado entre as partes mediante a assinatura do correspondente Contrato de Prestação de Serviços.

A fim de cumprir o seu objetivo, esta Política será revisada no mínimo a cada 2 (dois) anos, sendo mantido o controle de versões, e circulada aos colaboradores para conhecimento e assinatura do Termo de Adesão.

Em caso de dúvidas ou necessidade de aconselhamento, o colaborador deve buscar auxílio junto ao Diretor de Compliance da **RI GESTORA**, devendo as questões de segurança cibernética serem tratadas com o Coordenador da área de Tecnologia da Informação.

CAPÍTULO II - PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

1. Acesso Restrito

A troca de informações entre os colaboradores da **RI GESTORA** deve sempre pautar-se 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. Em caso de dúvida a área de compliance deve ser acionada previamente à revelação.

Os colaboradores da **RI GESTORA** que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos.

Os arquivos da Sociedade são armazenados em nuvem e servidores internos geridos pela área de TI / Administrativo.

O acesso controlado às pastas e arquivos se dá mediante a outorga de senhas de acesso individuais e intransferíveis que permitem a identificação do seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

Adicionalmente, todas as mensagens enviadas/recebidas dos computadores disponibilizados pela **RI GESTORA** permitem a identificação do seu remetente/receptor.

O acesso remoto pelos colaboradores é protegido por criptografia, pois o sistema se baseia na identidade do usuário, solicitando uma identificação – caso essa pessoa não tenha autorização para acesso, o documento, que é criptografado, não será exibido.

O armazenamento de informações protegidas em dispositivos portáteis deve restringir-se aqueles fornecidos pela Sociedade.

A outorga e cancelamento de senhas é de responsabilidade do TI, sempre mediante orientação do Diretor Compliance, a quem compete a verificação da estrutura de governança da **RI GESTORA**, a fim de evitar a transgressão de barreiras de informação e potenciais conflitos de interesse. Este procedimento deverá ser observado ainda na hipótese de mudança de atividade/área de um determinado profissional dentro da **RI GESTORA**.

As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança, devendo ser desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

Após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela Sociedade expiram, usando um protetor de tela protegido por senha que exige que a sessão somente possa ser reiniciada depois que o usuário tenha se autenticado novamente.

No caso do desligamento ou saída de algum colaborador, o acesso aos arquivos será automaticamente bloqueado e a respectiva senha revogada. Para sistemas externos, a **RI GESTORA** deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.

O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros das demais áreas de atuação da **RI GESTORA**, assim como de empresas do grupo econômico. O mesmo é aplicável à equipe de consultoria de valores mobiliários que encontra-se instalada em sala segregada e de acesso restrito somente à sua própria equipe e ao Diretor de Compliance.

2. Backup

Todos os documentos arquivados nos computadores da **RI GESTORA** são objeto de backup diário com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

O prestador de serviço na nuvem armazena versões anteriores de arquivos por até 30 dias, ou seja, se algum arquivo for apagado ou alterado de forma errônea, é possível recuperá-lo durante este período.

Os e-mails excluídos são mantidos na Lixeira por 180 dias. Após este período, a mensagem será excluída e somente o administrador poderá recuperá-la através da console de administração. Neste caso, serão mais 30 dias até que a mensagem seja definitivamente excluída sem a possibilidade de recuperação.

3. Cópia de Arquivos e Instalações

Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

A cópia de arquivos e instalação de programas em computadores deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

É terminantemente proibido que os colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da **RI GESTORA**. Nestes casos, o colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Sociedade. É vedada, ainda, a manutenção destes em mesas, máquinas de fax ou copiadoras.

4. Descarte de Informações

O descarte de informações confidenciais deve observar as seguintes diretrizes:

(i) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;
(ii) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;
(iii) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada;
(iv) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Sociedade devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

5. Redundância

Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe-chave, previamente designada e treinada para tanto, poderá acessar as informações na nuvem de qualquer local.

No tocante ao acesso à internet, a **RI GESTORA** dispõe de duas conexões banda larga ligadas simultaneamente pelo Firewall, que permite a automática comutação e a

divisão do tráfego para o serviço secundário, sempre que houver interrupção do serviço principal.

Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho e o servidor estão conectados a um equipamento do tipo no-break, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuários salvem seus arquivos.

O sistema de telefonia possui redundância via outra operadora.

CAPÍTULO III - SUPORTE E MONITORAMENTO

Em caso de pane da rede ou em alguma estação de trabalho, o fato deverá ser imediatamente comunicado à área de TI, que assegurará o suporte interno ou providenciará que seja acionado o suporte externo necessário.

O sistema eletrônico utilizado pela **RI GESTORA** está sujeito à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar

qualquer irregularidade na transferência de informações, seja interna ou externamente.

Nesse sentido, tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores, a **RI GESTORA** também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos colaboradores.

Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve ser objeto de informação ao Compliance para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

1. Tratamento de casos de vazamento de informações confidenciais

No caso de vazamento de informações confidenciais relacionadas aos clientes da **RI GESTORA**, ainda que oriundo de ação involuntária, o Diretor de Compliance notificará os interessados sobre o ocorrido.

Sem prejuízo, a **RI GESTORA** acionará o seu Plano de Recuperação visando a identificação da causa que ensejou o vazamento e responsabilização do causador. Ademais, será elaborado um Relatório acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

Este Relatório será elaborado pelo Diretor de Compliance e será submetido à Diretoria da **RI GESTORA** que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

2. Firewall

A **RI GESTORA** faz o uso da tecnologia de Firewall para proteger sua rede contra ameaças externas. O modelo utilizado é o NETGATE que inclui todas as funcionalidades de bloqueio de entrada.

3. Rede Wireless

A Sociedade possuí 2 (duas) redes WIFI distintas, uma para uso interno e outra para uso dos visitantes. Jamais deve ser divulgada a senha de acesso interno para os visitantes. Os visitantes devem sempre solicitar a senha de acesso para a recepcionista.

A rede WIFI para visitantes é bloqueada para acessar recursos internos.

4. Testes de Segurança

3.12. São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

ROTINAS OPERACIONAIS	PERIODICIDADE
Varredura de antivírus	Tempo real
Controle de conteúdo de Internet pelo Firewall e Antivírus	Tempo real
Varredura de memória pelo Antivírus	Tempo real
Autenticação de rede	Tempo real
Bloqueio de tela do Windows por Inatividade	A cada 10 minutos
Backup Online	Diário
Back Up Servidor	Diário
Atualizações nas estações de trabalho	Conforme demanda do sistema operacional
Troca da senha dos usuários	A cada 45 dias

CAPÍTULO IV - IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS CIBERNÉTICOS

Considerando que para o devido exercício das atividades de gestão profissional de recursos de terceiros de consultoria de valores mobiliários são essenciais todos os recursos tecnológicos necessários ao processo de análise, investimento e desinvestimento, tais como: (i) disponibilização das informações diárias sobre os fundos sob gestão; (ii) boletagem de operações; (iii) compra e venda de ativos para as carteiras sob gestão; (iv) conferência e liberação das carteiras diárias dos fundos sob gestão.

São estes:

I. Lote 45 e Atlas PAS.
II. SIGA (Itaú), Intrag Custódia (Intrag – Ativos), S3 Ativos e e-mail.
III. Bloomberg, Reuters, CETIP Trader e e-mail.
IV. Lote 45 e Atlas PAS

Abaixo são descritos os riscos internos identificados e respectivas avaliações. Para tanto, considerou-se:

I. Possíveis ameaças;
II. Grau de exposição dos ativos supramencionados às ameaças;
III. Impactos financeiros, operacionais e reputacional
IV. Expectativa de que o evento de segurança se efetive:

Risco Interno	Avaliação Inicial
Usuários que precisam de perfil administrativo na máquina local executem acidentalmente algum phishing, malware ou adware	Verificação dos logs do servidor de gerenciamento do antivírus, e avaliação da real necessidade de perfil administrativo.

Risco Externo	Avaliação Inicial
A empresa disponibiliza acesso remoto para a rede interna, somente para funcionários autorizados junto a Administração da **RI GESTORA**.	Todas as portas de entrada são bloqueadas no firewall com liberação administrativa apenas para o IP da equipe de TI e o acesso remoto pelos funcionários autorizados, é exclusivo em suas estações de trabalho, e com autenticação através de servidor Gateway.

CAPÍTULO V - AÇÕES DE PROTEÇÃO E PREVENÇÃO AOS RISCOS CIBERNÉTICOS

Os planos de ação e prevenção descritos neste Capítulo tem por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

Neste sentido, a **RI GESTORA** ratifica a adoção de controles de acesso físico e lógico implementados em linha com a Política de Segurança da Informação adotada. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da **RI GESTORA**, evitando o acesso por terceiros não autorizados.

Isto posto, todos os colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede, bem como às barreiras da informação com relação a outras atividades desempenhadas pela **RI GESTORA** ou empresas do mesmo grupo econômico.

Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência ou inadequação com relação aos acessos recomendados pelo Diretor de Compliance reportados imediatamente. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de colaboradores.

São adotadas as seguintes medidas preventivas para cada risco identificado:

Risco Interno	Ação de Proteção/Prevenção
Troca de senhas entre usuários	Bloqueio do usuário para acesso somente na própria estação de trabalho

Risco Externo	Ação de Proteção/Prevenção
Os sistemas são somente utilizados na rede interna da Sociedade.	

Todos os novos equipamentos e sistema instalados na **RI GESTORA** devem contar com as configurações de proteção acima descritas, sendo realizado teste em ambientes de homologação e de prova antes do início da sua utilização. Sem prejuízo, semestralmente são realizadas inspeções visando a verificação da atualização dos sistemas operacionais e softwares instalados nos computadores da Sociedade.

Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática, sendo vedadas aplicações não autorizadas por meio de controles de execução de processos.

CAPÍTULO VI - MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA

São realizados os seguintes testes de verificação para fins de identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados:

Rotina	Periodicidade
Backup	Diário
Teste de restauração de dados	Diário
Teste de invasão externa e phishing	30 dias

Teste de resposta a incidentes com simulação de cenários	30 dias
Análise de Logs e trilhas de auditoria	30 dias

São mantidos inventários atualizados de hardware e softwares utilizados pela **RI GESTORA**. Semestralmente são realizadas verificações, a fim de identificar elementos estranhos à **Sociedade**, tais como computadores não autorizados ou softwares não licenciados.

Sempre que houver alteração relevante na estrutura tecnológica da **RI GESTORA** serão realizadas análises de vulnerabilidade.

CAPÍTULO VII - RESPOSTAS A INCIDENTES CIBERNÉTICOS

A Sociedade adota os seguintes planos de ação de resposta a incidentes em função das ameaças identificadas:

Ameaça Interna	Severidade (Classificação)	Plano de Ação
Usuários que precisam de perfil administrativo na máquina local executem acidentalmente algum	1	Assim que recebido o log de infecção o equipamento é isolado da rede e é feita a remoção

phishing, malware ou adware		do software malicioso ou até mesmo a formatação do equipamento

Ameaça Externa	Severidade (Classificação)	Plano de Ação
Não se aplica		

Compete ao Compliance a comunicação da contingência aos demais colaboradores da **RI GESTORA**, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e severidade da contingência, em observância do Plano de Continuidade de Negócios.

Cabe ao Compliance a elaboração de relatórios acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente. Tais relatórios deverão ser submetidos à Diretoria da **RI GESTORA** que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a **RI GESTORA** estudará procedimentos preventivos a serem implementados e incluídos neste plano de continuidade de negócios.

CAPÍTULO VIII - PROGRAMA DE TREINAMENTO

A **RI GESTORA** conta com um programa de treinamento dos colaboradores que tenham acesso a informações relevantes sobre a **RI GESTORA**, seus negócios ou clientes.

Os procedimentos e rotinas definidos na presente Política serão abordados em treinamento anual, coordenado pelo Diretor de Compliance ou terceiro contratado para esta finalidade, visando a sua disseminação entre a equipe da **RI GESTORA**.

Poderão ser promovidos treinamentos em periodicidade menor, visando a atualização e ampliação do conhecimento dos colaboradores, em especial em

virtude de mudanças relevantes nos procedimentos e controles descritos nesta Política.

CAPÍTULO IX - DISPOSIÇÕES GERAIS E ENFORCEMENT

Todos os documentos, relatórios e informações relevantes para os procedimentos e rotinas descritos nesta Política são arquivados em meio físico ou eletrônico na **RI GESTORA**, pelo prazo mínimo de 5 (cinco) anos.

O presente Instrumento prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores da **RI GESTORA** aos seus termos e condições.

A título de *enforcement*, vale notar que a não observância dos dispositivos da presente Política resultará em advertência, suspensão, demissão ou exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.