POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
3ª REVISÃO
INÍCIO DA VIGÊNCIA
Jan/2021

CAPITÂNIA S/A

Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é o conjunto de procedimentos que devem ser seguidos para preservar a segurança, integridade e confidencialidade da informação sob gestão da Capitânia S/A.

A utilização das informações e meios de veiculação de informações da Companhia, incluindo computadores, telefones, internet, impressora e e-mail, deve ser feito sempre de forma diligente, ética e profissional.

Os servidores são conectados a nobreaks de 3 (três) KVA com autonomia de 2 (duas) horas, com desligamento automático do servidor via serial. Além disso, o edifício possui gerador próprio com autonomia para 4 (quatro) horas de modo a mitigar problemas de falhas elétricas com consequente perda de informação.

O Local do CPD (centro de processamento de dados) é exclusivo e climatizado, com acesso por senha.

Área de Tecnologia da Informação: Quanto à gestão de segurança da informação, serão responsabilidades específicas da área:

i Classificar os meios de informação computadorizados que administra, quanto à relevância, provendo condições mínimas necessárias de continuidade, disponibilidade e integridade desses;

ii Custodiar e administrar meios de informação informatizados, em uso ou de propriedade da Capitânia, tais como: notebooks, tablets, desktops, servidores, redes de computadores, mídias, softwares, hardwares, aparelhos de telefone, sistemas de informação, bases e bancos de dados, periféricos, provedores de internet, website, intranet e outros relacionados com tecnologia;

iii Homologar novos produtos de tecnologia (equipamentos, sistemas e *softwares*) de acordo com as regras e melhores práticas em segurança das informações;

iv Definir critérios e condições (uso, horários, prevenção a acidentes e incidentes), bem como monitorar acesso e manutenção do *data center*;

v Assegurar que exista um processo estruturado para registrar e informar os incidentes e violações de segurança em tecnologia da informação;

vi Assegurar que existam processos para a identificação e verificação dos registros de atividades, "logs" em todos os sistemas e recursos de tecnologia e dados;

vii Seguir procedimentos rígidos que garantam a base tecnológica para recuperação de desastres e continuidade dos negócios da Capitânia;

viii Fornecer suporte técnico especializado a todos os colaboradores;

ix Fornecer apoio técnico especializado aos Comitês de Segurança da Informação na elaboração do planejamento da estrutura e dos recursos que envolvam tecnologia;

x Gerenciar processos de mudanças e de retorno à normalidade (na eventualidade de crises, incidentes e emergências que acarretem o acionamento do Plano de Continuidade do Negócio);

xi Assegurar a gravação telefônica dos ramais necessários e o *backup* diário de informações, mantendo em arquivo seguro e organizado durante os prazos legais e/ou internos;

xii Zelar pelo uso e segurança, bem como o armazenamento interno e externo das mídias de *backup* durante os prazos internos definidos e os dispostos em leis, normas e regulamentos;

xiii Manter a confidencialidade das informações que tenham acesso; e

xiv Garantir a confidencialidade, disponibilidade e integridade das informações armazenadas nos equipamentos, sistemas e bases de dados da Capitânia.

Classificação da informação:

É de responsabilidade do Gerente/Supervisor, responsável de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

i Pública: É uma informação da Companhia ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

ii Interna: É uma informação da Capitânia que não há interesse em divulgar, na qual o acesso por parte de indivíduos externos à empresa deve ser evitado. Na hipótese desta informação ser acessada indevidamente, há risco de danos à imagem da Capitânia, porém, não com a mesma magnitude de uma informação confidencial. A informação interna pode ser acessada sem restrições por todos

os empregados e prestadores de serviços da empresa, quando não restrita a uma determinada área.

iii Confidencial: É uma informação crítica para os negócios da Capitânia ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à organização ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

iv Restrita: É toda informação que pode ser acessada somente por usuários da Capitânia explicitamente indicados pelo nome ou por área a qual pertencem. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Controles das Informações Confidenciais e Restritas:

Na condução de suas atividades profissionais, os colaboradores da Capitânia poderão obter informações de caráter confidencial e restritas sejam elas da própria empresa, dos colaboradores, dos clientes, ex-clientes, potenciais clientes ou mesmo referentes aos ativos detidos pelas carteiras dos fundos geridos pela gestora.

Considera-se "Informação Confidencial" todas e quaisquer informações e/ou dados de natureza confidencial (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à Capitânia, suas atividades e seus clientes e quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividade de administração de ativos e carteiras de valores mobiliários desenvolvida pela companhia, mesmo que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às transações aqui contempladas.

As Informações Confidenciais não incluem informações que sejam ou venham a se tornar de domínio público sem violação do disposto nesta política. Caso haja dúvida sobre o caráter confidencial de determinada informação, aquele que a ela teve acesso deve imediatamente relatar tal fato ao Diretor de Risco e Compliance.

A manutenção do estrito sigilo sobre as informações confidenciais ou restritas que forem confiadas a Capitânia e seus colaboradores aplica-se a informações obtidas via documentos físicos ou digitais, informações obtidas através de conversas, ainda que adquiridas no curso das atividades dos colaboradores.

Nenhuma informação confidencial poderá ser divulgada fora da Companhia, exceto nos casos descritos abaixo, devendo ainda ser divulgada internamente apenas em casos autorizados ou necessários para a realização adequada das atividades.

Informações confidenciais e ou restritas sobre clientes, ex-clientes ou potenciais clientes somente poderão ser compartilhadas:

(i) Dentro da Capitânia, conforme a necessidade para a condução dos negócios;

(ii) Com empresas cujo compartilhamento de determinadas informações sejam necessárias para atender aos clientes, ex-clientes ou potenciais clientes; avaliando a necessidade, o motivo e finalidade do compartilhamento. O Diretor de Risco e Compliance deve ser consultado previamente para a aprovação.

(iii) Com os reguladores e/ou quando exigido por lei, norma, regulamentos ou ordem judicial emitida por um tribunal de jurisdição competente, ou por um órgão, judiciário, administrativo ou legislativo; desde que, o Diretor de Risco e Compliance seja consultado previamente para aprovação.

Quaisquer exceções envolvendo o compartilhamento de informações confidenciais de clientes, ex-clientes ou potenciais clientes com pessoas não autorizadas deverão ser enviadas ao Diretor de Risco e Compliance para revisão e aprovação prévia.
O compartilhamento de informações da Capitânia, inclusive sobre sua estratégia de investimento, sistemas, remuneração e propriedade intelectual somente deverá ser feito com o entendimento expresso de que estas informações são confidenciais e devem ser utilizadas exclusivamente para a finalidade para o qual foram recebidas ou concedidas. As informações confidenciais devem ser utilizadas para fins profissionais apenas e sob nenhuma hipótese para obtenção de quaisquer vantagens pessoais. Toda pessoa que tiver acesso à informação nos termos desta política deverá obrigatoriamente assinar o "Termos de Confidencialidade e Sigilo" disponível no Anexo C.

Procedimentos internos para tratar eventual vazamento de informações confidenciais, reservadas ou privilegiadas.

Não obstante todos os procedimentos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Capitânia, na eventualidade de ocorrer o vazamento de quaisquer informações, ainda que de forma involuntária, a área de Compliance deverá tomar ciência do fato tão logo seja possível. De posse da informação, o Compliance, primeiramente, identificará se a informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas e operações. Nestes casos, o compliance procederá com o tanto necessário para cessar a disseminação da informação ou atenuar os seus impactos, conforme o caso.

O Diretor de Risco e Compliance responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da Capitânia, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial); e

(vii) Determinação do responsável que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Risco e Compliance, após a condução de investigação e avaliação completa das circunstâncias do incidente, para tanto, poderá, dentre outras medidas autorizado pelo Comitê de Compliance e Risco: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação.

I- Acesso aos Recursos de Informação

1. Senha de Login na Rede: Pessoal e intransferível.

    a. Cada usuário é responsável por todas as atividades realizadas por intermédio de sua senha de acesso. Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar à Capitânia em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação e nas normas e procedimentos específicos dela decorrentes.

b. Troca de senha requerida a cada 90 dias.

2. Acesso às Pastas: Todo arquivo de trabalho deve estar em uma das pastas do servidor central. Arquivos de trabalho no drive local (C:) não são permitidos, com exceção do arquivo .pst do Microsoft Outlook, por razões técnicas.

3. Programas: Todo programa só pode ser instalado pela área de Tecnologia. As requisições devem ser direcionadas a equipe de tecnologia e em cópia o Diretor de Risco e Compliance.

4. Equipamentos: Todo equipamento (monitores, computadores, laptops notebooks, switches, roteadores, caixas de som, impressoras entre outros) só pode ser instalado pela área de Tecnologia.
   Os computadores podem ser inspecionados a qualquer tempo para a verificação da observância do disposto na presente política;

5. E-mail: Deve ser utilizado apenas para atividades profissionais.
   Pastas de e-mail diferentes da Inbox ("pastas pessoais" no jargão Microsoft) devem ser armazenadas na rede, no diretório U: ("usuários"), sob a pasta pessoal.

6. Acesso à Internet: Deve ser utilizado apenas para atividades profissionais. Proibido:

   a. o acesso a conteúdo pornográfico, jogos, relacionamentos, conteúdo de hackers, proxys, conteúdo racista ou discriminatório de qualquer natureza.

   b. a utilização de softwares P2P e torrent como Emule, Kazaa, Vuze e outros.

   c. Download de filmes, músicas, seriados, jogos, softwares.

   O acesso à Internet é monitorado e sujeito a filtros de conteúdo.

   Qualquer liberação de acesso a sites deverá ser feita por escrito e estará sujeita a aprovação da área de Tecnologia e Gerente de Área por e-mail.

   A verificação do AntiSpam e antivírus é realizada diariamente.

7. Skype: Apenas Contas Designadas têm acesso autorizado ao Skype. É proibido:

   a. Postar mensagens de cunho discriminatório, difamatório, ou de qualquer maneira ilegal;

   b. Representar a Capitânia fora da função específica a que se destina.

8. Pen Drive: Apenas Usuários Designados têm pen-drive liberado.

9. Dispositivos de impressão: há um dispositivo de impressão por área. Cada estação deve mapear exclusivamente o dispositivo de impressão da sua área, exceto as usuários designados para ter acesso à impressora de alta qualidade

10. Impressora de Alta Qualidade: Localizada na Administração. Apenas usuários designados podem mapear esta impressora. Uso da mesma requer autorização da área de Compliance.

11. Acesso remoto à rede da Capitânia: Apenas usuários designados podem ter acesso à VPN. Devido a potencial vulnerabilidade da estação remota, o uso deve ser parcimonioso, liberado com configuração pela TI e autorizado pelo gestor da área. Além do VPN, a Capitâna possui outras ferramentas de acesso remoto que provem o acesso a todos os Colaboradores (Anydesk, Team Viewer, Chrome Remote Desktop).

12. Usuários Designados: São aqueles listados no Anexo A.

13. Certificação Digital: Apenas os diretores, assim definidos em Estatuto Social podem assinar em nome da Capitânia. Para isso, a mesma disponibiliza aos colaborador assinatura digital login de acesso e senha. Login, senha e token são pessoais e intransferíveis.

II- Política de Backup

1. Serviços de backup são:

    a. Backup InSite: incremental, criptografado, diário por 12 meses, com finalidade de recuperar arquivos acidentalmente perdidos.
    São utilizados backup em disco rígido para uma melhor tolerância a falhas.

    b. Backup para o Site de Contingência: diário, para site remoto, via VPN, com a finalidade de restaurar a operação após parada do site principal.

    c. Backup OffSite: backup para disco rígido removível (criptografado, protegido por senha), armazenado em dois locais diferentes do site principal e do site de contingência.

    d. Backup de e-mail no servidor: realizado em ambiente cloud protegido por senha e aplicação própria de comunicação entre servidor e caixa de e-mail (comunicação em túnel). Sistema de backup de mensagens sem limite de tamanho e número de mensagens.

2. Os arquivos PST (Personal Storage Table) dos usuários são copiados semanalmente para um disco rígido externo criptografado e armazenado em local diferente do site de contingência e do site principal.

3. Em nenhuma circunstância os equipamentos de Backup OffSite e site de Contingência poderão estar ao mesmo tempo no site principal. Para uma total reestruturação após evento catastrófico deverá ser utilizado sistema de rodízio para reestabelecer o ambiente.

III- Plano de Continuidade de Negócios

Planos de contingência:

Plano	Descrição
1. Link de Contingência	Link de internet redundante acionado automaticamente em caso de queda do link principal e ainda trabalhando em paralelo para que não haja um estrangulamento de conexão.
2. Contingência de e-mail	Contas de e-mail hospedadas em ambiente Cloud com 99,995% de uptime garantido por contrato.
3. Queda de energia	No-breaks instalados em todas as máquinas e servidores e em caso de queda, um gerador assume a distribuição de energia.
4. Site de Contingência	Site independente em caso de disrupção grave do site principal. Site independente com copias de segurança dos arquivos do site principal.
5. Telefonia	Além das linhas telefônicas contratadas (E1) existem ainda linhas externas independentes do PABX ligadas ao gerador

1. Site de Contingência- Está localizado distante do site principal e será composto de:

    a. Instalações físicas para 4 estações;

    b. Acesso banda larga à internet com firewall;

    c. Servidor sincronizado com o site principal, com defesas contra acesso não autorizado (senha de criptografia e firewall);

    d. Rede para pelo menos 4 estações.

e. Impressora

f. Pelo menos 1 desktop além do servidor.

2. Serviços do Site de Contingência contam com no mínimo:

   a. Sistema SMA – WEB;

   b. Arquivos Administrativos;

   c. Arquivos e diretórios que possibilitam a continuidade dos trabalhos da empresa, tais como planilhas e documentos.

3. Serviços Remotos de Contingência acessíveis remotamente serão:

   a. E-mail (webmail e smartphone)

4. Rotinas essenciais: a serem executadas do site de contingência:

   a. Envio diário de cota para investidores;

   b. Atividades de backoffice offsite referentes a operacioanalização das carteiras geridas;

   c. Trabalhos referentes ao *"core business"* da empresa.

5. Ordem de Ativação:

   a. Com queda da energia do site principal antes que as rotinas essenciais tenham sido completadas, faz-se ativação dos no-breaks automaticamente e antes que a bateria dos mesmos seja exaurida, o gerador deverá assumir a distribuição de energia.

   b. O site de contingência (remoto) deve ser ativado se:

      i. Houver impossibilidade física de acessar o site principal; ou

      ii. Não houver possibilidade de ligação à internet no site principal (nenhum dos links, principal ou contingência, e nenhum meio viável de acesso por modem de celular); ou

      iii. A manutenção do site principal sob queda de energia tiver atingido o limite máximo dos nobreaks e gerador; ou

      iv. Rotinas necessárias envolverem os servidores e estes não estiverem disponíveis.

6. Procedimento de Ativação – Site Contingência.

    a. Mover para o site de contingência o número necessário de pessoas com laptops (menos 1 estação já provida no site)

    b. Conectar na rede (usar rede wireless se o número de conexões passar de 4) – atenção para a senha de conexão de rede wireless disponível no site.

    c. Mapear as pastas do servidor de contingência conforme necessário.

IV- Rotinas de Testes

7. Teste do site de Contingência:

    a. Aleatoriamente, com frequência esperada trimestral, as rotinas essenciais (liberação de quota, boletagem, home broker, envio de relatórios) deverão ser feitas do Site de contingência.

8. Teste de gravação de Telefonia:

    a. Diariamente, será verificada a taxa de gravação dos arquivos à procura de anomalias (arquivos crescendo rápida ou lentamente demais);

    b. Semanalmente, deve ser testada a gravação nas salas de reunião;

9. Teste de No-Break e Gerador

    a. Trimestralmente a energia do escritório deverá ser cortada para se verificar a disponibilidade e autonomia dos nobreaks e gerador;

    b. Semestralmente será feita manutenção preventiva nos equipamentos de energia ou caso algum deles apresente defeito nos testes trimestrais;

    c. Semestralmente o gerador deverá ser verificado quanto ao seu reservatório de combustível.

10. Teste de equipe de segurança

    a. Aleatoriamente, com frequência esperada trimestral e em horários aleatórios o alarme deverá ser disparado para verificar o tempo de resposta e qualidade de reposta, visto que nem sempre a contrassenha será fornecida.

b. Trimestralmente um funcionário aleatório em um final de semana deverá acessar o prédio sem que seu nome esteja na lista de permissões.

11. Teste de Backup

a. Mensalmente o backup deverá ser recuperado (restore) de uma pasta selecionada aleatoriamente.

b. Semestralmente deverá ser feito uma recuperação completa dos arquivos da empresa.

12. Alteração de senhas de acesso

a. Trimestralmente as senhas de acesso aos conjuntos deverão ser alteradas.

V- Gravação de Comunicações

1. A CAPITÂNIA monitorará o tráfego de informações através de suas redes de comunicação, ou seja, telefonia, internet e correio eletrônico.

2. Os ramais de telefonia gravados são:

a. Todos os Ramais

3. O conteúdo das gravações será transferido do servidor de gravação para:

a. HD externo removível criptografado protegido por senha com periodicidade de 6 meses.

4. O acesso a gravações só pode ser realizado com permissão da pessoa gravada, ou quando exigido por lei.

5. Comunicações via Skype são gravadas em pasta na rede por programa residente específico.

6. Os acessos feitos pela internet são gravados pelo servidor, com identificação do usuário que acessou e o destino acessado.

VI- Segregação de Informação

1. Áreas de Segregação: As seguintes são áreas estanques:

a. Consultoria;

b. Asset.

2. Licenças: A Capitânia Consultoria e Serviços Ltda opera sob licença de Consultor de Valores Mobiliários; A Gestão de Carteira opera sob licença de Administrador de Carteiras de Valores Mobiliários; ambas emitidas pela CVM.

3. Segregação Física: Cada área se comunica única e exclusivamente com o Hall de saída (Recepção / Elevadores). Não existem janelas, salas de reunião ou visita ou outras áreas comuns. As salas de visita constituem bloco à parte ligado à Recepção e ao Hall de saída. Cada uma das áreas fica em um conjunto separado com porta com senha própria.

4. Segregação Lógica: as partições do servidor de arquivo terão acesso exclusivo por área e por perfil de usuário.

5. Mapeamentos:
   É disponibilizado um diretório que é de uso comum e deve conter exclusivamente material comum (pesquisa, biblioteca, acesso ao Bloomberg). Quaisquer arquivos estranhos a estas denominações deverão ser movidos para suas pastas especificas sob o risco de serem deletados (Pasta Geral sem informação sensível).

   Os equipamentos de roteamento (*switches*, roteadores, *hubs*) que servem cada área devem ser independentes.

6. Segregação Funcional: associados não podem ter função em mais de uma área.

7. Segregação de Informações: associados de uma área não podem trocar informações confidenciais, proprietárias ou não-públicas da área com associados de outra área.

VII- Revisão da política

1. Todas as políticas acima listadas deverão ser revistas em um prazo máximo de 12 meses após a conclusão de sua aplicação.

   a. Tal revisão deverá ser feita com o intuito de atualizar a mesma aos novos riscos apresentados durante o período por uma série de fatores, sejam eles comportamentais (novo tipo de celular, óculos inteligentes, discos externos etc..), físicos, cibernéticos (ataques a roteadores, impressoras ou novas modalidades de ataques a servidores) ou por conta de políticas empresariais e de compliance.

VIII- Treinamento

1. Corporativo: É obrigatório treinamento interno em segurança da informação, negociação por detentores de informação privilegiada, e segregação de informação, pelo menos uma vez por ano. A frequência é obrigatória. Cada participante deve assinar uma declaração de que participou do treinamento, conforme modelo no Anexo B.

2. Corporativo de TI: Treinamentos recorrentes das melhores práticas de segurança, novidades e mudanças na área de TI que poderá influenciar diretamente os funcionários.

3. Equipe de TI: Treinamento e atualização da equipe de TI em termos de melhores práticas de segurança, recursos e novidades.

CONSIDERAÇÕES FINAIS

Em caso de desligamento do colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações. Caberá a equipe de TI ações como cancelamento da conta de email, rede e retirada de acessos.

O Diretor de Risco e Compliance será o responsável pela aplicação desta política, como também pelo monitoramento do uso das informações pelos colaboradores da Capitânia.

Para assegurar o fiel cumprimento de suas regras internas, bem como da legislação em vigor, a Capitânia se reserva o direito de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas vias internet, intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), bem como os arquivos armazenados ou criados pelos recursos da informática pertencentes à Companhia ou utilizados em nome dela.

ANEXO A

Usuários Designados

Nome	Pen-Drive	Acesso Remoto	VPN	Impressora Qualidade	Partição Administrativa
Ricardo Quintero (quintero)	X	X		X	X
César Lauro (clauro)	X	X		X	X
Margareth Brisolla (mbrisolla)	X	X		X	X
Arturo Profili (arturo)	X	X		X	
Flávia Krasupenhar (flavia)	X	X		X	
Camila Lupino		X	X	X	
Carlos Fernandes	X	X	X	X	
Christopher Smith		X		X	
Camila Souza		X		X	
Rafael Piccinini da Silva	X	X		X	X
Caio Conca		X		X	
Fábio Cabral Góes		X		X	
Carlos Simonetti		X		X	
Gustavo Moura		X		X	
Pedro Lobo		X		X	
Leonardo Moreira Salles		X			
Andréia Goldspan		X			
Lucieli Andrade		X	X		

ANEXO B

Modelo de DECLARAÇÃO DE PARTICIPAÇÃO

DECLARAÇÃO DE PARTICIPAÇÃO NO TREINAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO

Eu, XXXXX, participei do Treinamento Interno de Segurança da Informação, versando sobre segurança da informação, confidencialidade, negociação por pessoas detentoras de informações privilegiadas, e segregação de atividades, oferecido pela Capitânia em ....., e me comprometo a aderir às melhores práticas apresentadas.

São Paulo, _____ de _____ de _____

ASSINATURA:

NOME:

ANEXO C – TERMO DE CONFIDENCIALIDADE E SIGILO

Eu,_____, inscrito(a) no CPF nº _____, reconheço que, em razão da minha atuação na Capitânia. ("Empresa"), estabelecerei contato com informações privadas da Sociedade, que são classificadas como restrita ou confidencial. Estas informações devem ser tratadas com absoluta reserva em qualquer condição e não podem ser divulgadas ou dadas a conhecer a terceiros não autorizados, sem a expressa e escrita autorização.

Desta forma, assumo o compromisso de manter confidencialidade e sigilo sobre todas as informações relacionadas as atividades da empresa, a que tiver acesso por força da minha relação com a Sociedade, nos termos da Política de Segurança de Informação e Informações Confidenciais.

Por este termo de confidencialidade e sigilo comprometo-me:

i. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;

ii. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;

iii. A não me apropriar de material confidencial e/ou sigiloso que venha a ser disponível;

iv. A não repassar o conhecimento das informações confidenciais, responsabilizando-me por todas as pessoas que vierem a ter acesso às informações, por meu intermédio, e obrigando-me, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

Neste Termo, as seguintes expressões serão assim definidas:

Considera-se "Informação Confidencial" todas e quaisquer informações e/ou dados de natureza confidencial (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à Sociedade, suas atividades e seus clientes e quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham ido direta ou indiretamente fornecidos ou divulgados em razão da atividade de gestão de ativos e carteiras de valores mobiliários desenvolvida pela Sociedade, mesmo que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às transações aqui contempladas.

As Informações Confidenciais não incluem informações que sejam ou venham a se tornar de domínio público sem violação do disposto na Política de Segurança da Informação.
Pelo fiel cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

São Paulo, ____/____/____

_____
Assinatura

São Paulo, 28 de dezembro de 2020.

_____	_____
Ricardo Quintero	César Lauro da Costa
Presidente	Vice-Presidente
_____	_____
Arturo Profili	Flávia Krauspenhar Siqueira Cunha
Diretor	Diretora
_____	_____
Caio Conca	Carlos Emanuel Simonetti
Diretor	Diretor
_____	_____
Margareth Brisolla	Rafael Piccinini da Silva
Diretora	Diretor