# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Capitânia Prev S.A.

Abril de 2024

# Sumário

# I. 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 Prev S.A ("**GESTORA**").

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.

Atualmente a **GESTORA** conta com links de internet e telefonia com redundância. A rede elétrica do parque tecnológico é contingenciada por um nobreak que atende à demanda do parque por cerca de uma hora. Os servidores estão hospedados em um cloud provider, para garantir o funcionamento contínuo das atividades em caso de indisponibilidade da rede do escritório físico, seja por algum problema de tecnologia, seja por indisponibilidade de acesso físico e/ou de infraestrutura predial. Os backups são realizados diariamente fora do horário do expediente. Os arquivos gerados são criptografados e armazenados em nuvem.

O Data Center da **GESTORA** fica localizado em uma sala restrita com acesso por senha e biometria e com acesso apenas ao departamento de Tecnologia.

Entretanto, caso em uma hipótese de contingência o Data Center se torne inacessível, a Política de Segurança da Informação e Cibernética prevê:

- O uso, pelos Colaboradores, de e-mail corporativo em nuvem (Works pace);
- O fornecimento, pela Capitânia, de equipamento de notebook para os Colaboradores designados, previamente formatado pela equipe de Tecnologia;
- A possibilidade de acesso remoto à todas as informações e dados armazenados no servidor físico, via VPN (Virtual Private Network) instalado nas máquinas de todos os colaboradores

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

- Classificar os meios de informação computadorizados que administra, quanto à relevância, provendo condições mínimas necessárias de continuidade, disponibilidade e integridade desses;
- Custodiar e administrar meios de informação informatizados, em uso ou de propriedade da **GESTORA**, 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;

- Homologar novos produtos de tecnologia (equipamentos, sistemas e softwares) de acordo com as regras e melhores práticas em segurança das informações;
- Definir critérios e condições (uso, horários, prevenção a acidentes e incidentes), bem como monitorar acesso e manutenção do data center;
- Assegurar que exista um processo estruturado para registrar e informar os incidentes e violações de segurança em tecnologia da informação;
- Assegurar que existam processos para a identificação e verificação dos registros de atividades, "logs" em todos os sistemas e recursos de tecnologia e dados;
- Seguir procedimentos rígidos que garantam a base tecnológica para recuperação de desastres e continuidade dos negócios da **GESTORA**;
- Fornecer suporte técnico especializado a todos os colaboradores;
- Fornecer apoio técnico especializado aos Comitês de Segurança da Informação na elaboração do planejamento da estrutura e dos recursos que envolvam tecnologia;
- 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);
- 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;
- 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;
- Manter a confidencialidade das informações que tenham acesso; e
- Garantir a confidencialidade, disponibilidade e integridade das informações armazenadas nos equipamentos, sistemas e bases de dados da **GESTORA**.

## II. 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:

- 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 dela.
- Interna: É uma informação da **GESTORA** 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 **GESTORA**, 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.
- Confidencial: É uma informação crítica para os negócios da **GESTORA** 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.
- Restrita: É toda informação que pode ser acessada somente por usuários da **GESTORA** 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.

## III. Controles das Informações Confidenciais e Restritas

Na condução de suas atividades profissionais, os colaboradores da **GESTORA** 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 **GESTORA**, 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 **GESTORA** 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:

- Dentro da **GESTORA**, conforme a necessidade para a condução dos negócios;
- Com empresas, cujo compartilhamento de determinadas informações seja necessário 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.
- 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 **GESTORA**, 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.

## IV. 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 **GESTORA**, na eventualidade de ocorrer o vazamento de quaisquer informações, ainda que de forma involuntária, a área de Risco e Compliance deverá tomar ciência do fato tão logo seja possível. De posse da informação, o Diretor de Risco e Compliance, primeiramente, identificará se a informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas e operações. Nestes casos, 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:

- 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;
- Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
- Determinação dos papéis e responsabilidades do pessoal apropriado;
- Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
- Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

- 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 **GESTORA**, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial); e
- 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 Risco e Compliance: (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.

## V. Acesso aos Recursos de Informação

- Senha de Login na Rede: Pessoal e intransferível.
    - 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 **GESTORA** em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação e nas normas e procedimentos específicos dela decorrentes.
    - Troca de senha requerida a cada 90 dias.
- Utilização de MFA (Múltiplo Fator de Autenticação) no acesso aos e-mails e ferramentas de nossa rede.
- 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.
- 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.
- 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;

- 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.
- Acesso à Internet: Deve ser utilizado apenas para atividades profissionais. Proibido:
  - O acesso a conteúdo pornográfico, jogos, site de apostas, relacionamentos, conteúdo de hackers, proxys, conteúdo racista ou discriminatório de qualquer natureza;
  - A utilização de softwares P2P e Torrent como uTorrent, BitTorrent, Delluge e outros;
  - 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 à aprovação da área de Tecnologia e Gerente de Área por e-mail.

  A verificação do AntiSpam e antivírus é realizada diariamente.

- Skype e Teams: Todos os colaboradores possuem acesso autorizado ao Skype. É proibido:
  - Postar mensagens de cunho discriminatório, difamatório, ou de qualquer maneira ilegal;
  - Representar a **GESTORA** fora da função específica a que se destina.
- Pen Drive: Apenas Usuários Designados têm pen-drive liberado.
- Dispositivos de impressão: há um dispositivo de impressão por área. Cada estação deve mapear exclusivamente o dispositivo de impressão da sua área, exceto os usuários designados para ter acesso à impressora de alta qualidade
- Acesso remoto à rede da **GESTORA**: Apenas usuários designados podem ter acesso à VPN. Devido a potencial vulnerabilidade da estação remota, o uso deve ser parcimonioso, liberado com configuração pela equipe de Tecnologia e autorizado pelo gestor da área. Além do VPN, a **GESTORA** possui outras ferramentas de acesso remoto que provem o acesso a todos os colaboradores (3 opções de ferramentas de acesso).
- Usuários Designados: São aqueles listados no Anexo A.

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

## VI. Política de Backup

- Serviços de backup são:
    - 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.
    - Backup para o Site de Contingência em um ambiente de Disaster Recovery (DR) via VPN, com a finalidade de restaurar a operação após parada do site principal.
    - 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.

## VII. Plano de Continuidade de Negócios

Plano de contingência:

| Plano | Descrição |
|---|---|
| 1. Link | 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. e-mail | Contas de e-mail hospedadas em ambiente Cloud com 99,995% de uptime garantido por contrato. |
| 3. Queda de energia | Nobreak instalado para atender todo parque de máquinas, servidores hospedados em cloud provider que permite o funcionamento ininterrupto. |

| | |
|---|---|
| 4. Site de Contingência | Site independente em caso de disrupção grave do site principal.<br>Site independente com copias de segurança dos arquivos do site principal. |
| 5. Telefonia | Telefonia hospedada na nuvem, permitindo o acesso ininterrupto do serviço, através de apps mobiles. |

- Site de Contingência - possui um ambiente de Disaster Recovery (DR) completo, em um cloud provider, com o objetivo de:
    - Garantir o funcionamento contínuo das atividades da **GESTORA** em caso de indisponibilidade da rede do escritório físico, seja por algum problema de TI, seja por indisponibilidade de acesso físico e/ou de infraestrutura predial
    - Replicar o Active Directory da **GESTORA** em uma nuvem privada;
    - Replicar online o File Server, para que em caso de ativação da contingência, a perda de informação seja limitada a pouquíssimos arquivos ainda não sincronizados;
    - Manter o mesmo nível de segurança da rede interna em caso de ativação do ambiente DR, e não criar nenhuma forma de aumento de exposição do risco de vazamento de informações da GESTORA. Além do ambiente de site replication, que permite subir um ambiente espelho ao do escritório da GESTORA, com as informações de logins e segurança e com os arquivos todos atualizados até segundos antes do Fail Over, existe também um serviço de backup em nuvem, com retenção de várias imagens dos arquivos, com a intenção de garantir a capacidade de restauração do ambiente em casos de ataques de Ramsonware, que prejudiquem tanto os arquivos da rede quanto suas cópias espelhadas no ambiente de Disaster Recovery.

## VIII. Rotinas de Testes

- Teste do site de Contingência:
    - Aleatoriamente, com frequência esperada trimestral, deve ser testado o DR;
- Teste de gravação de Telefonia:
    - Diariamente, será verificada a taxa de gravação dos arquivos à procura de anomalias (arquivos crescendo rápida ou lentamente demais);

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

- Teste de Nobreak
  - Trimestralmente a energia do escritório deverá ser cortada para se verificar a disponibilidade e autonomia dos nobreaks;
  - Semestralmente será feita manutenção preventiva nos equipamentos de energia ou caso algum deles apresente defeito nos testes trimestrais;
- Teste de equipe de segurança
  - 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.
  - Trimestralmente um funcionário aleatório em um final de semana deverá acessar o prédio sem que seu nome esteja na lista de permissões.
- Teste de Backup
  - Mensalmente o backup deverá ser recuperado (“restore”) de uma pasta selecionada aleatoriamente.
- Alteração de senhas de acesso
  - Trimestralmente as senhas de acesso aos conjuntos deverão ser alteradas.

## IX. Gravação de Comunicações

- A **GESTORA** monitorará o tráfego de informações através de suas redes de comunicação, ou seja, telefonia, internet e correio eletrônico.
- Os ramais de telefonia gravados são:
  - Todos os Ramais
- As gravações são efetuadas diretamente em cloud provider (AWS):
- O acesso a gravações só pode ser realizado com permissão da pessoa gravada, ou quando exigido por lei.
- Comunicações via Skype e Teams são gravadas em pasta na rede por programa residente específico.

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

## X. Segregação de Informações

- Áreas de Segregação: As seguintes são áreas estanques:
    - Consultoria;
    - Gestoras;
- Licenças: A Capitânia Prev S.A. opera sob licença sob licença de Administrador de Carteiras de Valores Mobiliários; emitida pela CVM.
- Segregação física: todas as áreas de comunicam uniformemente com a hall de saída (Recepção / Elevadores). Salas de reunião ou salas de visitas constituem um departamento a parte ligado à Recepção e ao Hall de saída
- Cada uma das áreas fica em um departamento separado.
- Segregação Lógica: as partições do servidor de arquivo terão acesso exclusivo por área e por perfil de usuário.
- Mapeamentos:

É disponibilizado um diretório que é de uso comum e deve conter exclusivamente material comum (pesquisa, biblioteca, acesso ao Bloomberg, Quantum). 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.

- Segregação Funcional: associados não podem ter função em mais de uma área.
- Segregação de Informações: associados de uma área não podem trocar informações confidenciais, proprietárias ou não-públicas da área com associados de outra área.

## XI. Revisão da Política

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

## XII. Treinamento

- 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.
- Corporativo de Tecnologia: Treinamentos recorrentes das melhores práticas de segurança, novidades e mudanças na área de Tecnologia que poderá influenciar diretamente os funcionários.
- Equipe de Tecnologia: Treinamento e atualização da equipe de Tecnologia em termos de melhores práticas de segurança, recursos e novidades.
- Utilização da Plataforma de Compliance BeCompliance e realização de treinamentos assim determinados pela área de Risco e Compliance.

## XIII. 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 Tecnologia ações como cancelamento da conta de e-mail, 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 **GESTORA**.

Para assegurar o fiel cumprimento de suas regras internas, bem como da legislação em vigor, a **GESTORA** 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 via 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.

## XIV. Aprovação e Revisão

| VERSÃO | DATA | ELABORADO / MODIFICADO POR | APROVADO POR |
|---|---|---|---|
| 3º | 30/04/2024 | Rico e Compliance | Diretoria de Risco e Compliance |

# XV. Anexo A – Usuários Designados

| Nome | Pen-Drive | Acesso Remoto | VPN | Impressora | Partição Administrativa |
|---|---|---|---|---|---|
| Adriano Ribeiro | | X | X | X | |
| Aldeni Araújo | | X | X | X | |
| Alexandre Alfer | | X | X | X | |
| Andreia Mendonça | | X | X | X | |
| Ariel Halaban | | X | X | X | |
| Arthur Castro | | X | X | X | |
| Arturo Profili | X | X | X | X | |
| Caio Conca | X | X | X | X | |
| Camila Lupino | | X | X | X | |
| Carlos Simonetti | X | X | X | X | |
| Carlos Fernandes | | X | X | X | |
| Cauã Santos | | X | X | X | |
| Cesar Lauro | X | X | X | X | X |
| Christopher Smith | | X | X | X | |
| Fabio Góes | | X | X | X | |
| Felipe Cateb | | X | X | X | |
| Felipe Silveira | | X | X | X | |
| Flávia Krasupenhar | X | X | X | X | |
| Francilene Silva | | X | X | X | |
| Gabriel Martins | | X | X | X | |
| Gustavo Moura | | X | X | X | |
| Gustavo Castilho | | X | X | X | |
| Izilda Damas | | X | X | X | |
| Jorge Machado | | X | X | X | |
| Leonardo Sales | | X | X | X | |
| Lucieli Andrade | | X | X | X | |
| Margareth Brisolla | X | X | X | X | X |
| Matheus Cavalcanti | | X | X | X | |
| Monik Dourado | | X | X | X | |
| Pedro Carvalho | | X | X | X | |
| Rafael Souza | | X | X | X | |
| Rafael Piccinini | | X | X | X | X |
| Raphael Costa | | X | X | X | |
| Ricardo Quintero | X | X | X | X | X |
| Rogério Lino | | X | X | X | |
| Samuel Gimenes | | X | X | X | |
| Thiago Furnielis | | X | X | X | |
| Vitor Pacheco | | X | X | X | |

# XVI. 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 Prev S.A., em ....., e me comprometo a aderir às melhores práticas apresentadas.

São Paulo, _____ de _____ de _____

_____

ASSINATURA:

NOME:

# XVII. Anexo C – Termo de Confidencialidade e Sigilo

Eu, _____, inscrito(a) no CPF nº _____, reconheço que, em razão da minha atuação na Capitânia Prev S.A. (“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:

- 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;
- A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;
- A não me apropriar de material confidencial e/ou sigiloso que venha a ser disponível;
- 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