Manual de Compliance, Ética e Controles Internos

Data da Atualização: 31/03/2022

Versão: 2022-01

Aprovado por: Ricardo Garcia (diretor)

E Andre Laport (diretor)

Data da Aprovação: 25/03/2022

VINLAND Capital Management
Gestora de Recursos Ltda.

VINLAND Capital Management International
Gestora de Recursos Ltda.

VINLAND Capital Management Crédito Privado
Gestora de Recursos Ltda.

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

Parte 2
Manual de compliance

1. Introdução

Este Manual de Compliance ("Manual") foi elaborado em conformidade com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014, na Instrução CVM n.º 558, demais orientações da CVM, no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA de ART") e no Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação") e se aplica a todos os Colaboradores da Vinland.

O presente Manual reúne as diretrizes que devem ser observadas pelos Colaboradores no desempenho da atividade profissional, visando ao atendimento de padrões éticos cada vez mais elevados. Este documento reflete a identidade cultural e os compromissos que a Vinland assume nos mercados em que atua.

Em caso de dúvidas ou necessidade de aconselhamento, é imprescindível que se busque auxílio imediato junto ao Diretor de Compliance, Risco e PLD da Vinland.

1.1. Ambiente Regulatório

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, ao assinar o termo de compromisso constante do Anexo I a este Manual, aceitam expressamente as normas aqui estabelecidas.

1.2. Termo de Compromisso

Todo Colaborador, ao receber este Manual, assinará um Termo de Compromisso (Anexo I). Pela assinatura deste documento, o Colaborador reconhece e confirma seu conhecimento e concordância com os termos deste Manual, bem como das demais políticas adotadas pela Vinland, que serão disponibilizadas juntas com o presente Manual no momento de integração do Colaborador com a Vinland, conforme descrito na Política de Treinamento.

Ao firmar o Termo de Compromisso, cada Colaborador compromete-se a zelar pela aplicação das condutas de compliance, princípios éticos e normas estabelecidas e contidas neste Manual e nas demais políticas da Vinland.

O descumprimento de quaisquer das regras estabelecidas neste Manual deverá ser levado para apreciação direta do Diretor de Compliance, Risco e PLD da Vinland. Ao tomar conhecimento do descumprimento de quaisquer regras, o Diretor de Compliance, Risco e PLD deverá tomar as medidas cabíveis para sanar eventual problema ocorrido, podendo levar a questão para os principais sócios da Vinland, caso entenda por necessário.

A Vinland não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso a Vinland venha a ser responsabilizada ou sofra prejuízos de qualquer natureza por atos de seus Colaboradores, a Vinland exercerá seu direito de regresso contra os responsáveis.

2. Política de confidencialidade

2.1. Termo de Confidencialidade

Conforme estabelecido no Termo de Responsabilidade e Confidencialidade (Anexo II), nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada à terceiros não Colaboradores da Vinland. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais.

Qualquer informação sobre a Vinland, seu know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos de investimento geridos pela Vinland, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela Vinland, estruturas, planos de ação, relação de clientes, contrapartes comerciais, Terceiros, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Vinland e/ou de seus sócios e clientes, obtida em decorrência do desempenho das atividades do Colaborador na, ou para a, Vinland, só poderá ser fornecida à terceiros, ao público em geral, aos meios de comunicação ou demais órgãos públicos ou privados se assim for previamente autorizado pelo Diretor de Compliance, Risco e PLD.

A informação obtida em decorrência da atividade profissional exercida na Vinland não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados, excetuando-se, por lógica, àquelas expressamente aprovadas pelo Diretor de Compliance, Risco e PLD. Enquadram-se neste item, por exemplo, posições compradas ou vendidas, estratégias de investimento ou desinvestimento, relatórios, estudos realizados (Research) – independentemente destas análises terem sido realizadas pela Vinland ou por terceiros – opiniões internas sobre ativos financeiros, informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes do fundos de investimento geridos pela Vinland, transações realizadas e que ainda não tenham sido divulgadas publicamente, além daquelas estabelecidas no Termo de Responsabilidade e Confidencialidade (Anexo II).

Na questão de confidencialidade e tratamento da informação, o Colaborador deve cumprir o estabelecido nos itens a seguir.

2.1.1. Informação Privilegiada

Considera-se Informação Privilegiada qualquer informação relevante a respeito de qualquer companhia, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros).

As Informações Privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

Quem tiver acesso a uma Informação Privilegiada deverá divulgá-la imediatamente ao Diretor de Compliance, Risco e PLD, não devendo divulgá-la a ninguém mais, nem mesmo a outros integrantes da Vinland, profissionais de mercado, amigos e parentes, e nem a utilizar, seja em benefício próprio ou de terceiros. Caso haja dúvida sobre o caráter privilegiado da informação, aquele que a ela teve acesso deve se abster

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

utilizar tal informação, seja em benefício próprio, de terceiros ou mesmo da Vinland e de seus clientes, bem como deve imediatamente relatar tal fato ao Diretor de Compliance, Risco e PLD. Todos aqueles que tenham acesso a uma informação privilegiada deverão, ainda, restringir totalmente a circulação de documentos e arquivos que contenham essa informação.

2.1.2. Informações Confidenciais

Sem prejuízo da definição de Informações Privilegiadas acima, são consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Manual, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Vinland sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da Vinland, incluindo:

(i) know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

(ii) informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Vinland;

(iii) operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela Vinland;

(iv) estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

(v) informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Vinland e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Vinland e que ainda não foi devidamente levado à público;

(vi) informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;

(vii) transações realizadas e que ainda não tenham sido divulgadas publicamente; e

(viii) outras informações obtidas junto a sócios, diretores, funcionários, trainees, estagiários ou jovens aprendizes da Vinland ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados.

2.1.3. Insider Trading, Divulgação Privilegiada e Front Running

Insider Trading consiste na compra e venda de títulos ou valores mobiliários com base na utilização de Informação Privilegiada, visando à obtenção de benefício próprio ou de terceiros, nos termos do artigo 27-D da Lei n.º 6.385, de 07 de dezembro de 1976, conforme alterada.

Divulgação Privilegiada é a divulgação, a qualquer terceiro, de Informação Privilegiada que possa ser utilizada com vantagem na compra e venda de títulos ou valores mobiliários.

Front Running é a prática de aproveitar alguma informação para concluir uma negociação antes de outros, inclusive no que tange à uma posição comprada ou vendida relevante em um determinado ativo que eventualmente alterasse as cotações do ativo negociado.

É vedada a prática de todos os procedimentos acima referidos por qualquer integrante da Vinland, seja atuando em benefício próprio, da Vinland, de seus clientes, ou de terceiros. Assim, deve ser observado o disposto nos itens de "Informação Privilegiada", Insider Trading, "Divulgação Privilegiada" e Front Running não só durante a vigência de seu relacionamento profissional com a Vinland, mas mesmo depois do seu término.

A utilização ou divulgação de "Informação Privilegiada", Insider Trading, "Divulgação Privilegiada" e Front Running, sujeitará os responsáveis às sanções previstas neste Manual, inclusive desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Vinland, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da Vinland, e ainda às consequências legais cabíveis.

2.2. Política de Conflito de Interesses e Segregação Das Atividades

A Vinland tem por objetivo o exercício da atividade de administração de carteiras de valores mobiliários, na categoria "gestora de recursos de terceiros", a qual é exaustivamente regulada pela CVM e autorregulada pela ANBIMA.

Desse modo, a Vinland reconhece que o Diretor Responsável pela administração de carteiras de valores mobiliários perante a CVM ("Diretor de Investimentos") não pode ser responsável por nenhuma outra atividade no mercado financeiro e de capitais, na instituição ou fora dela.

A atividade de gestão de recursos exige credenciamento específico e está condicionada a uma série de providências, dentre elas a segregação total de suas atividades de gestão de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas (com exceção da distribuição de cotas de fundos de investimento que é gestora, conforme regulamentação em vigor) pela Vinland ou empresas controladoras, controladas, ligadas ou coligadas, bem como prestadores de serviços.

Neste sentido, a Vinland informa que:

(a) a VINLAND Capital Management Gestora de Recursos Ltda, a VINLAND Capital Management International Gestora de Recursos Ltda. e a VINLAND Capital Management Crédito Privado Gestora de Recursos Ltda. são sociedades que se encontram sob o mesmo controle, constituídas e autorizadas pela CVM para atuarem como administradoras de carteiras de valores mobiliários na categoria "gestoras de recursos", cuja prestação de serviços desta natureza se dá, preponderantemente, por meio da gestão de fundos de investimentos;

(b) Tendo em vista a natureza diversa de seus mercados de atuação e a ausência de potenciais conflitos de interesses

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

estruturais, as Gestoras Vinland poderão atuar de forma unificada do ponto de vista operacional, de risco, compliance e controles internos, conforme permitido pela legislação em vigor; e

(c) Nesse mesmo sentido, o Diretor de Investimentos e o Diretor de Compliance, Risco e PLD atuam concomitantemente em tais funções em todas as Gestoras Vinland, em linha com a faculdade do artigo 4º parágrafo 4º da Instrução CVM nº 558.

Adicionalmente, os normativos aplicáveis não vedam a existência de potenciais conflitos de interesse, mas obrigam os participantes do mercado a estabelecer mecanismos de mitigação de potenciais conflitos de interesse e a endereçá-los para a ciência da CVM, dos investidores e das empresas atuantes no mercado que venham a se relacionar com a Vinland.

Com efeito, nos termos da regulamentação em vigor, a imposição da segregação de forma compulsória é apenas e tão somente devida entre a área responsável pela administração de carteiras de valores mobiliários e as áreas responsáveis pela intermediação e distribuição de valores mobiliários que não de fundos próprios.

Nesse sentido, as Gestoras Vinland informam que, apesar da existência de Colaboradores em comum entre si, fato é que as Gestoras Vinland estabeleceram regras e restrições, conforme dispostas ao longo das políticas que integram o Manual de Ética e Controles Internos, especialmente do item 2.4. abaixo, para mitigar o risco do uso indevido de Informações Confidenciais as quais os Colaboradores possam ter acesso.

Desse modo, as Gestoras Vinland, sempre que aplicável, assegurarão aos Colaboradores, seus clientes e às autoridades reguladoras, a completa segregação de suas atividades, adotando procedimentos operacionais objetivando a segregação física de instalações entre as Gestoras Vinland e outras empresas responsáveis por diferentes atividades prestadas no mercado de capitais.

2.3. Barreiras de Informação

Os Colaboradores detentores de Informações Confidenciais, em função de seu cargo devem estabelecer uma barreira de informações com os demais colaboradores. O Diretor de Investimentos e o Diretor de Compliance, Risco e PLD devem manter o registro dos Colaboradores que detenham Informações Confidenciais, com a indicação do tipo de informação detida.

Essas barreiras servem para atender a diversos propósitos, incluindo a conformidade com leis e regulamentos que governam o tratamento e a utilização de certos tipos de informação; evitar situações que possam suscitar um potencial conflito de interesses ou a má utilização de informações. Via de regra, a Vinland deverá manter barreiras de informações físicas e eletrônicas adequadas e necessárias a consecução de suas atividades.

2.4. Barreiras de Informações Relacionadas a Informações Internas

Certas barreiras de informações gerenciam o fluxo de Informações Confidenciais internas (informações relevantes de caráter privado) para evitar sua divulgação ou má utilização. Essas barreiras de informações restringem o compartilhamento de informações internas entre Colaboradores de estratégias de gestão distintas.

Essas barreiras incluem também a divisão física e eletrônica entre os negócios das diferentes equipes de gestão e restringem o acesso a sistemas de computador e a alguns sites dedicados da Intranet. Além disso, a Área de Compliance e Risco adota lista de ativos que devem ser observados (Watch List), bem como proíbe operações por todos os gestores relacionados a determinado ativo ou emissor (Restricted List), na hipótese de participação da Vinland em negociações relacionadas a informações materiais e não públicas, as quais são atualizadas e divulgadas periodicamente aos Colaboradores.

3. Política de treinamento

3.1. Treinamento Inicial

A Vinland possui um processo de integração e treinamento inicial dos seus Colaboradores e um programa de treinamento contínuo de tais Colaboradores com relação aos princípios gerais e normas de compliance da Vinland descritas neste Manual, bem como às principais leis e normas aplicáveis às suas atividades, conforme preceitua a Instrução CVM n.º 558.

Assim que cada Colaborador passa fazer parte do dia a dia da Vinland, antes do início efetivo de suas atividades, ele participará de um processo de integração e treinamento onde irá adquirir conhecimento sobre as atividades da Vinland, suas atribuições e normas internas, políticas e códigos, além de informações sobre as principais leis e normas que regem as atividades da Vinland.

A referida integração trata de um treinamento cujo objetivo é passar a filosofia da Vinland, bem como adequar o Colaborador ao estilo profissional e particular da Vinland. Logo, ao iniciar suas atividades em nossa instituição, o Colaborador receberá todas as políticas da Vinland, bem como uma explicação sobre as diretrizes da Vinland, devendo, nessa ocasião, assinar os documentos anexo ao presente Manual de forma a atestar a ciência e concordância com a cultura os procedimentos internos da Vinland.

3.2. Treinamento Contínuo

Adicionalmente ao Treinamento Inicial, cujos procedimentos se encontram descritos no item acima, a Vinland entende que é fundamental que todos os Colaboradores tenham conhecimento, bem como mantenham-no sempre atualizado, dos seus princípios éticos, bem como das leis e normas aplicáveis às atividades da instituição.

Neste sentido, em cumprimento a referida norma e aos valores da nossa instituição, a Vinland adota um programa de treinamento contínuo dos seus Colaboradores, com o objetivo de fazer com que os mesmos estejam sempre atualizados sobre os termos e responsabilidades que estão sujeitos.

O referido programa de treinamento contínuo dos Colaboradores da Vinland consiste, dentre outras atividades, na disponibilidade do Diretor de Compliance, Risco e PLD para tirar quaisquer dúvidas dos Colaboradores a qualquer momento, com o intuito de manter os Colaboradores sempre em consonância com as regras dos órgãos reguladores, autorreguladores e da própria Vinland.

A Vinland também irá, no mínimo, realizar um treinamento anual aos seus Colaboradores, de temática e duração a serem definidos pela Área de Compliance e Risco.

Este documento foi assinado digitalmente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

Ademais, em caso de alguma alteração nas políticas da Vinland, devido à exigência de órgãos reguladores ou por outros motivos, a Vinland poderá realizar um programa de treinamento para os Colaboradores, com o intuito de fornecer o novo Manual ou a(s) nova(s) política(s) aos mesmos e também de apresentar as mudanças e os novos pontos abordados.

Por último, cumpre salientar que todos os processos de treinamento (inicial, contínuo e eventual) são controlados pelo Diretor de Compliance, Risco e PLD e exigem o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

4. Política de segurança cibernética

4.1. Conceito

A Política de Segurança Cibernética da Vinland estabelece diretrizes aplicáveis a todos os Colaboradores da Vinland.

Os Colaboradores devem cumprir as exigências desta Política de Segurança Cibernética e, além disso, assumem a responsabilidade profissional de agir de maneira ética em todos os atos que pratiquem.

Para fins da Política de Segurança Cibernética, serão aplicadas as definições listadas Parte 1 – Código de Ética do presente Manual da Vinland, salvo se outro significado lhes for expressamente atribuído neste documento.

Adicionalmente ao disposto no presente documento, serão aplicadas as políticas do prestador de serviços de TI (Norma de Utilização de Recursos da Rede Corporativa e Diretrizes de Segurança da Informação) desenvolvidos para a Vinland.

4.2. Objetivos

Esta Política de Segurança Cibernética visa proteger os equipamentos, sistemas e dados de propriedade e/ou uso da Vinland ("Recursos" ou "Infraestrutura de TI") contra fraudes, uso indevido, ataque de cibercriminosos, perda ou sequestro de dados.

O acesso, o uso indevido ou não autorizado dos referidos ativos da Vinland é tratado na Política de Segurança da Informação, parte integrante do presente Manual.

4.3. Responsabilidades

4.3.1. Da Diretoria

(i) Direcionar os esforços e recursos propostos para a segurança da informação, de acordo com a estratégia de negócios da empresa;

(ii) Aprovar as normas de segurança da informação e suas atualizações;

(iii) Aprovar os controles a serem utilizados para garantir a segurança das informações;

(iv) Acompanhar os indicadores de segurança e os incidentes reportados pela empresa prestadora de serviços de TI;

(v) Comunicar Diretor de Compliance, Risco e PLDao Diretor de Compliance, Risco e PLD os casos de violações das Políticas Internas relativas à informação para as providências necessárias;

(vi) Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados;

(vii) Aprovar o planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação; e

(viii) Delegar as funções de segurança da informação aos profissionais responsáveis.

4.3.2. Da Empresa Prestadora de Serviços de Infraestrutura

(i) Monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;

(ii) Orientar os testes da infraestrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;

(iii) Assessorar as demais áreas da empresa no processo de classificação das informações;

(iv) Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios específico de cada uma;

(v) Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;

(vi) Identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;

(vii) Manter a infraestrutura que suporta o ambiente controlado;

(viii) Manter a infraestrutura e sistemas atualizados;

(ix) Garantir a implementação e operação dos indicadores de segurança;

(x) Notificar imediatamente os incidentes de segurança a diretoria; e

(xi) Garantir a rápida tomada de ações em caso de incidentes de segurança.

4.3.3. Do Diretor de Compliance, Risco e PLD

(i) Desenvolver, manter e implementar programas de treinamento e de conscientização aos Colaboradores sobre as normas de segurança da informação, a forma como ela está estruturada e os principais conceitos de segurança da informação;

(ii) Gerenciar os problemas disciplinares resultantes de violações dos controles de segurança da informação juntamente com os gestores dos envolvidos;

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

(iii) Emitir o Termo de Compromisso, conforme Anexo I deste Manual;

(iv) Gerenciar a assinatura do Acordo de Confidencialidade quando da contratação de terceiros ou prestadores de serviços, conforme modelo;

(v) Em conjunto com a Administração, determinar as sanções cabíveis de acordo com a legislação em vigor;

(vi) Revisar periodicamente a Política de Segurança da Informação e sugerir as alterações necessárias.

4.4. Identificação de Riscos (risk assessment)

No âmbito de suas atividades, a Vinland identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Vinland, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pela Vinland e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Vinland; e
- Governança da Gestão de Risco: a eficácia da gestão de risco pela Vinland quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Vinland identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- *malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware e Ransomware*);
- engenharia social – métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);
- ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- invasões (advanced persistent threats): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Vinland avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

4.5. Equipamentos

Os equipamentos objeto desta Política de Segurança Cibernética são os de propriedade da Vinland, tais como desktops, monitores, teclados, mouses, telefone, impressoras, desfragmentador de papéis e outros destinados ao uso pessoal ou comum dos Colaboradores da Vinland.

Eles deverão ser utilizados exclusivamente para fins profissionais e estão sujeitos à monitoramento periódico pela Diretor de Compliance, Risco e PLD, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual, sendo que seu uso indevido está sujeito às penalidades previstas no Código de Ética. Desta forma, o Diretor de Compliance, Risco e PLD poderá utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

Em caso de quebra ou indisponibilidade de equipamento (desktops, telefone), estarão disponíveis para uso imediato os equipamentos de contingência pré-configurados.

Nas hipóteses em que for necessário acionar uma infraestrutura replicada - física ou virtualizada - que garanta a substituição de um servidor, roteador, nobreak e/ou outro equipamento de TI que falhe ou esteja inacessível (Redundância de TI) entrará em operação a Política de Continuidade dos Negócios da Vinland.

4.6. Instalações elétricas e o sistema de refrigeração

A fim de assegurar as condições ideais de funcionamento da Infraestrutura de TI, evitando perda de dados por falta ou sobrecarga de energia ou superaquecimento; e danos aos equipamentos de informática, é imprescindível instalações elétricas e sistema de refrigeração adequados.

Ambos foram dimensionados de acordo com a estrutura instalada sob orientação de profissionais especializados.

4.7. Funcionamento contínuo dos Recursos de TI

Os Recursos de TI em sistema no-stop será feito por nobreak, que garante o funcionamento da infraestrutura por tempo suficiente para que nenhuma informação seja perdida quando ocorre falta de energia elétrica por até 3 horas. Os critérios de funcionamento e o procedimento para realização dos testes de verificação estão descritos na Política de Continuidade dos Negócios.

4.8. Firewall

As intrusões ou invasões são praticadas por pessoas que pretendem acessar, roubar ou sequestrar dados confidenciais e/ou informações privilegiadas, capturar dados para realização de fraudes, causar danos a sistemas e aplicativos.

A fim de evitar esses riscos, a Vinland conta com um mecanismo de controle do tráfego de dados entre os computadores de uma rede interna e desses com redes externas ("Firewall"). Ele trabalha segundo protocolos de segurança que garantem o correto funcionamento da comunicação entre as duas pontas, visando impedir intrusões.

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

Seu funcionamento é contínuo, as atualizações são programadas e realizadas automaticamente pelo sistema.

4.9. Senhas

A Vinland adota uma estrutura e configuração que induz a criação de senhas fortes, a fim de dificultar o acesso de pessoas mal-intencionadas em seus sistemas. Há, ainda, um mecanismo automático que obriga a alteração periódica de senhas pelos usuários ativos e cancela as senhas de usuários inativos/desligados da organização.

4.10. Softwares

A Vinland possui as licenças de uso de todos os softwares que utiliza. A Administração é responsável pelas renovações nos prazos e termos definidos em cada contrato.

É proibido o download e instalação de aplicativos de qualquer natureza ou procedência sem o consentimento da Diretor de Compliance, Risco e PLD.

O backup periódico de dados da rede, sua abrangência, armazenagem, metodologia e periodicidade é descrito na Política de Continuidade dos Negócios.

4.11. Correspondências eletrônicas

Apenas os Colaboradores e sócios da Vinland possuirão conta de e-mails corporativas, que serão criadas pela empresa responsável pela Infraestrutura de TI no momento da contratação ou integralização de cotas sociais.

O responsável pela conta de e-mail individual ou do departamento deverá lhe atribuir uma senha de acesso pessoal, sigilosa e intransferível.

Essas correspondências poderão ser acessadas para fins de monitoramento pela Diretor de Compliance, Risco e PLD.

Em caso de desligamento do Colaborador ou retirada do sócio, o acesso ao respectivo e-mail será imediatamente bloqueado pelo profissional de TI por orientação do Diretor de Compliance, Risco e PLD.

Os e-mails serão armazenados pela Microsoft, que proverá também os serviços de antisspam, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de Informações Confidenciais e Privilegiadas.

4.12. Armazenamento de dados em nuvem

Com vistas a evitar a perda de informações proprietárias, confidenciais e/ou privilegiadas, a Vinland adota a armazenagem automática de dados em nuvem.

4.13. Telefone

A Vinland definirá os Colaboradores que terão acesso à linha telefônica corporativa de acordo com a atividade que desempenharão.

O uso do telefone deverá se restringir às atividades profissionais em prol da Vinland e estará sujeita à gravação automática, para fins de monitoramento e confirmação de operações.

O monitoramento será feito periodicamente à critério do Diretor de Compliance, Risco e PLD, mediante acesso ao portal de telefonia contratado, a fim de fazer cumprir o Código de Ética.

4.14. Erros de procedimentos internos

Procedimentos de gestão da segurança da informação mal estruturados ou desatualizados podem acarretar vulnerabilidades e perdas de dados. Essas vulnerabilidades se manifestam por falhas no desenvolvimento, na implementação ou na configuração de mecanismos de segurança em softwares, no funcionamento dos hardwares ou em exposição a ameaças previsíveis.

A Vinland conta com equipe especializada para a execução dos protocolos de manutenção e segurança de seus Recursos de TI, como apontado acima.

4.15. Crises ou situações críticas

Na hipótese de situações não rotineiras em que os mecanismos descritos nesta Política de Segurança Cibernética se tornarem insuficientes ou ficarem indisponíveis, será acionada a Política de Continuidade dos Negócios, no que couber.

5. Política de segurança da informação

5.1. Introdução

A Política de Segurança da Informação da Vinland é documento que orienta e estabelece as diretrizes corporativas da Vinland para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

5.2. Objetivos

A Política de Segurança da Informação tem por objetivo estabelecer diretrizes que permitam aos seus Colaboradores seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo, bem como nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Ademais, a Vinland entende essencial preservar as informações que tenha acesso, sobretudo, quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

5.3. Aplicações da Política de Segurança da Informação

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

As diretrizes aqui estabelecidas deverão ser seguidas por todos os Colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta Política de Segurança da Informação dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada Colaborador se manter atualizado em relação a esta Política de Segurança da Informação e aos procedimentos e normas relacionadas, buscando orientação do Diretor de Compliance, Risco e PLD quando não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

5.4. Princípios da Política de Segurança da Informação

Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pela Vinland pertence à referida empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos Colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

5.5. Requisitos da Política de Segurança da Informação

O Diretor de Compliance, Risco e PLD da Vinland será responsável por prever as regras e normas aqui estabelecidas, bem como a sua revisão e ampla comunicação a todos os Colaboradores da Vinland.

A Política de Segurança da Informação deverá ser revista e atualizada periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de Compliance, Risco e PLD.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos Colaboradores. Todos os Colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar o Termo de Responsabilidade e Confidencialidade, anexo a este Manual.

Ainda, cabe salientar os Colaboradores tem a obrigação de atuar para que todo incidente que afete a segurança da informação deva ser comunicado inicialmente ao Diretor de Compliance, Risco e PLD.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Vinland julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, smartphones, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros ou por terceiros.

A Vinland exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta Política de Segurança da Informação será implementada na Vinland por meio de procedimentos específicos, obrigatórios para todos os Colaboradores, independentemente do nível hierárquico ou função instituição, bem como de vínculo empregatício ou prestação de serviços.

O não cumprimento dos requisitos previstos nesta Política de Segurança da Informação acarretará violação às regras internas da empresa e sujeitará o usuário às sanções administrativas e legais cabíveis.

5.6. Das responsabilidades

1 - Da Gestão de Tecnologia e Segurança da Informação

O Diretor de Compliance, Risco e PLD, enquanto responsável pela presente Política de Segurança da Informação, ou outro Colaborador indicado por esse, com o auxílio da equipe terceirizada de TI realizará as seguintes atividades:

- Testar a eficácia dos controles utilizados e informará aos principais sócios os riscos residuais.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança da Informação.
- Segregar as funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Vinland.
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.
- O Diretor de Compliance, Risco e PLD deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada.
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
- Os usuários (login) individuais de funcionários serão de responsabilidade do próprio funcionário.
- Os usuários (login) de terceiros serão de responsabilidade do diretor da área contratante.
- Proteger continuamente todos os ativos de informação da Vinland contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Vinland em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Vinland.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Vinland.
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos da Vinland;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Vinland;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e
- Atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Vinland.
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Vinland, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

2 - Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta Política de Segurança da Informação, a Vinland poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Diretor de Compliance, Risco e PLD;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

5.7. Testes Periódicos de Segurança em Sistemas de que Controlam Informações Confidenciais

Na Vinland, o acesso aos todos os sistemas, incluindo os que controlam Informações Confidenciais, é liberado com base no princípio da necessidade da informação para a execução de função (need-to-know/need-to-have principle). O controle é feito por meio dos perfis de acesso, que segregam as funções. Cada colaborador possui um conjunto de perfis relacionados às suas atividades, e a Vinland dispõe de controles internos para que o acesso seja liberado mediante aprovação. Todos os colaboradores recebem treinamento sobre segurança da informação e assinam o termo de ciência da Política de Segurança da Informação. A Vinland oferece avaliações e treinamentos periódicos aos quais os colaboradores são submetidos durante o ano, com o objetivo de conscientizá-los sobre confidencialidade das informações, cyber segurança, engenharia social, phishing, entre outras potenciais ameaças à integridade dos sistemas de informação, além da conscientização sobre essas ameaças e de como se proteger delas e responder a elas.

Nesse sentido, a Vinland realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Vinland e circulem em ambientes externos à Vinland com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Vinland. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Adicionalmente, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Vinland qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Vinland dispõe de tecnologias de defesa contra possíveis ataques aos seus sistemas e realiza testes periódicos no sistema disponível na rede mundial de computadores (SITE), denominados Penetration Test, que são executados por um terceiro especializado. Estes testes são realizados anualmente com os próprios colaboradores, que são submetidos a uma simulação de phishing.

A efetividade da Política de Segurança da Informação será verificada por meio de testes periódicos dos controles existentes, portanto um plano de teste deve ser efetuado pelo responsável por TI. A fim de verificar a integridade dos sistemas, inclusive com relação aos sistemas de Informações Confidenciais mantidas em meio eletrônico, a equipe de TI realiza testes semestrais, que são formalizados por meio de um reporte enviado ao Diretor de Compliance, Risco e PLD. Semestralmente a equipe de TI confirmará com os respectivos coordenadores de cada Colaborador a lista de todos os sistemas ao qual possuem acesso e os coordenadores deverão confirmar se os acessos devem ser mantidos a cada um desses sistemas.

O reporte a ser enviado ao Diretor de Compliance, Risco e PLD deverá conter a lista de todos os sistemas e respectivos colaboradores que possuem acesso, juntamente com a confirmação dos respectivos coordenadores, além de eventuais inconsistências detectadas em cada sistemas.

O Plano de testes assegura que:

1. Os recursos humanos e computacionais estejam adequados ao porte e as áreas de atuação;

2. Adequado nível de confidencialidade e acessos as Informações Confidenciais;

3. Segregação lógica de dados;

4. Recursos computacionais, de controle de acesso físico e lógico, estejam protegidos; e

5. Manutenção de registros que permita a realização de auditorias e inspeções.

O Diretor de Compliance, Risco e PLD deverá revisar a lista, confirmando a adequação dos acessos de cada Colaborador e adotando eventuais medidas cabíveis para correção das inconsistências detectadas.

Adicionalmente, o descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Com o intuito de identificar os colaboradores detentores de Informação Confidencial para responsabilização em caso de vazamento, serão e instituídos controles apropriados, trilhas de auditoria, registros de atividades, em todos os pontos e sistemas em que a Vinland julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, smartphones, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros ou por terceiros. Ainda, serão implementados controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

As atividades dos Colaboradores que utilizarem os sistemas e máquinas de propriedade da Vinland estão sujeitas à verificação, inclusive no que se refere aos acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros), para tanto, a Vinland instalou sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

5.8. Correio Eletrônico

O uso do correio eletrônico da Vinland é para fins corporativos e relacionados às atividades do Colaborador dentro da empresa. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Vinland e não cause impacto no tráfego da rede. A Vinland proíbe expressamente seus Colaboradores quanto ao uso do correio eletrônico da Vinland para as seguintes atividades:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Vinland;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Vinland vulnerável a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a Vinland estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
- contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Vinland;
- contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- contenha arquivos com código executável ou qualquer outra extensão que represente um risco à segurança;

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

- vise obter acesso não autorizado a outro computador, servidor ou rede;
- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar Informações Confidenciais sem explícita autorização do proprietário;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política); e
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Ainda, as mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do Colaborador
- Departamento
- Nome da empresa
- Telefone (s)
- Correio eletrônico

5.9. Internet

Todas as regras atuais da Vinland visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da empresa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Vinland, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo superior. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a empresa cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela empresa aos seus Colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos na Vinland.

Apenas os Colaboradores autorizados pela Vinland poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais. Nesse sentido, é proibida a divulgação e/ou o compartilhamento indevido de Informações Confidenciais em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela equipe terceirizada de TI.

Ainda, como regra geral, materiais de cunho sexual ou que representem perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Eventuais exceções poderão ser reportadas formalmente ao Diretor de Compliance, Risco e PLD e serão por ele analisadas.

5.10. Identificação

Os dispositivos de identificação e senhas protegem a identidade do Colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Vinland e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (artigo 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os Colaboradores.

Todos os dispositivos de identificação utilizados na Vinland, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a empresa e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um Colaborador, a responsabilidade perante a Vinland e a legislação (cível e criminal) será dos usuários que dele se utilizarem.

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

É proibido o compartilhamento de login para funções de administração de sistemas.

A Área de Recursos Humanos da Vinland é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos Colaboradores.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 9 (nove) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Diretor de Compliance, Risco e PLD da Vinland.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, A Área de Recursos Humanos da Vinland deverá imediatamente comunicar tal fato a equipe terceirizada de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

5.11. Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos Colaboradores são de propriedade da Vinland, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Vinland, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do Diretor de Compliance, Risco e PLD da Vinland, ou de quem este determinar. As áreas que necessitarem fazer testes deverão solicitá-los previamente ao Diretor de Compliance, Risco e PLD, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a equipe terceirizada de TI mediante registro de chamado junto ao Diretor de Compliance, Risco e PLD.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Vinland (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Os documentos imprescindíveis para as atividades dos Colaboradores deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os Colaboradores da Vinland não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do Diretor de Compliance, Risco e PLD.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha para restringir o acesso de Colaboradores não autorizados. Tais senhas serão definidas pela equipe terceirizada de TI da Vinland, que terá acesso a elas para manutenção dos equipamentos.
- Os Colaboradores devem informar ao Diretor de Compliance, Risco e PLD da Vinland, por meio formal, qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da equipe terceirizada de TI da Vinland ou por terceiros devidamente contratados para o serviço.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir invasão/evasão de informações, programas, vírus. Em

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização do Diretor de Compliance, Risco e PLD.

- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- O Colaborador deverá manter a configuração do equipamento disponibilizado pela Vinland, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da Vinland.
- Todos os recursos tecnológicos adquiridos pela Vinland devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

5.12. Dispositivos Móveis

A Vinland deseja facilitar a mobilidade e o fluxo de informação entre seus Colaboradores. Por isso, permite que eles usem dispositivos portáteis. Por "dispositivo portátil" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da empresa, ou aprovado e permitido pelo Diretor de Compliance, Risco e PLD, como: notebooks, smartphones e pen-drives.

A Vinland, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança. Os Colaboradores devem se abster de utilizar dispositivos portáteis que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Vinland.

Ainda, o Colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Vinland, mesmo depois de terminado o vínculo contratual mantido com a Vinland.

O suporte da equipe terceirizada de TI aos dispositivos móveis de propriedade da Vinland e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela empresa.

Todo Colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização do Diretor de Compliance, Risco e PLD e sem a condução, auxílio ou presença de um técnico da equipe terceirizada de TI.

O Colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da equipe terceirizada de TI da Vinland. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela Vinland constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

O Colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará que assumiu todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a Vinland e/ou a terceiros.

5.13. Data Center

O acesso ao Data Center somente deverá ser feito por sistema forte de autenticação. Todo acesso ao Data Center, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Adicionalmente, deverá ser executada semestralmente uma auditoria nos acessos ao Data Center por meio do relatório do sistema de registro. O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura.

A lista de funções com direito de acesso ao Data Center deverá ser constantemente atualizada e salva no diretório de rede. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um Colaborador autorizado. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer Colaborador responsável pela administração de liberação de acesso.

A chave da porta do Data Center deverá ficar na posse do Diretor de Compliance, Risco e PLD, ou Colaborador definido por este. O Data Center deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a autorização do Diretor de Compliance, Risco e PLD.

A entrada ou retirada de quaisquer equipamentos do Data Center somente se dará com o preenchimento da solicitação de liberação pelo Colaborador solicitante e a autorização formal desse instrumento pelo Diretor de Compliance, Risco e PLD.

No caso de desligamento de Colaboradores que possuam acesso ao Data Center, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de Colaboradores autorizados.

5.14. Revisão

O Diretor de Compliance, Risco e PLD realizará uma revisão da Política de Segurança da Informação e da Política de Segurança Cibernética a cada 24 (vinte e quatro) meses, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Vinland e acontecimentos regulatórios relevantes.

6. Política de anticorrupção

6.1. Conceito

Seguindo os preceitos da Lei n.º 12.846, de 1º de agosto de 2013 ("Lei Anticorrupção"), bem como os de sua regulação, através do Decreto n.º 8.240, de 18 de março de 2015, o combate à corrupção é um dever da Vinland e de todos os seus Colaboradores.

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

A Lei Anticorrupção responsabiliza as pessoas jurídicas, nos âmbitos administrativo e civil, pelos atos lesivos previstos praticados em seu interesse ou benefício e não exclui a responsabilidade individual de seus dirigentes ou administradores ou de qualquer pessoa natural, autora, coautora ou partícipe do ato ilícito. Desta forma, qualquer violação desta Política de Anticorrupção e da Lei de Anticorrupção pode resultar em penalidades civis e administrativas severas para a Vinland e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

Os atos lesivos poderão ser praticados contra a administração pública, nacional ou estrangeira, que para fins desta Política de Anticorrupção serão considerados, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

Adicionalmente, quanto a administração pública estrangeira considera-se os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados "agentes públicos" para os propósitos desta Política de Anticorrupção e da Lei de Anticorrupção.

6.2. Atos Lesivos e Sanções

De forma a tornar mais claro todas as condutas a serem evitadas pelos Colaboradores, a Vinland elenca abaixo os atos lesivos à administração pública, conforme interpretação do referido diploma legal:

(a) Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

(b) Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nesta lei;

(c) Comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

(d) No tocante a licitações e contratos: (i) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público; (ii) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público; (iii) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; fraudar licitação pública ou contrato dela decorrente; (iv) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo; (v) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou (vi) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública; e

(e) Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

Ainda pela Lei de Anticorrupção, as sanções previstas para a pessoa jurídica responsabilizada pelos atos ilícitos apresentados anteriormente são:

I. Perdimento dos bens, direitos ou valores que representem vantagem ou proveito direta ou indiretamente obtidos da infração, ressalvado o direito do lesado ou de terceiro de boa-fé;

II. Suspensão ou interdição parcial de suas atividades;

III. Dissolução compulsória da pessoa jurídica;

IV. Proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas e de instituições financeiras públicas ou controladas pelo poder público, pelo prazo mínimo de 1 (um) e máximo de 5 (cinco) anos.

Adicionalmente as condutas descritas acima, é terminantemente proibido dar ou oferecer qualquer valor ou presente a agente público sem autorização prévia do Diretor de Compliance, Risco e PLD, o que irá caracterizar violação a Lei de Anticorrupção e ensejar a aplicação das penalidades previstas nestas, mesmo que a oferta de suborno seja recusada pelo agente público.

Ainda, os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal o u regulamentar.

Nenhum sócio ou colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

Ademais, A Vinland garante que não fará, em hipótese alguma, doação a candidatos e/ou partidos políticos via pessoa jurídica. Em relação às doações individuais dos Colaboradores, a Vinland e seus Colaboradores têm a obrigação de seguir estritamente a legislação vigente.

Por fim, quando se fizer necessária a realização de reuniões ou audiências ("Audiências") com agentes públicos, sejam elas internas ou externas, a Vinland será representada por, ao menos, 2 (dois) Colaboradores, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar a Vinland contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a Vinland deverão elaborar relatórios de tais Audiências, e apresentá-los ao Diretor de Compliance, Risco e PLD imediatamente após sua ocorrência.

6.3. Procedimentos e Programa de Integridade

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

A Vinland utiliza seus melhores esforços para monitorar todos os Colaboradores da instituição, de forma a garantir que atuem em observância à Lei Anticorrupção e sua regulamentação, respeitando e praticando, na medida de suas atividades e possibilidades, os atos referentes ao Programa de Integridade disposto no Decreto n.º 8.240, de 18 de março de 2015.

Tal monitoramento é fundamental, pois também é responsabilidade de todos os Colaboradores proteger a empresa de atividades de corrupção e suborno, de forma que não serão tolerados comportamentos omissos sobre a questão ou envolvimento nesses tipos de atividade.

Diante disso, constituem parâmetros do programa de integridade da Vinland as seguintes medidas:

(a) Comprometimento dos sócios da Vinland com as práticas de compliance e controles internos;

(b) Políticas de conduta e ética que são aplicadas para todos os Colaboradores da Vinland, inclusive a terceiros, quando necessário;

(c) Treinamento periódico dos Colaboradores;

(d) Registros contábeis que reflitam as transações da Vinland de forma precisa e completa, feitos por empresa especializada externa;

(e) Independência dos procedimentos de compliance;

(f) Espaços para comunicação de irregularidades por meio de quaisquer Colaboradores ou terceiros;

(g) Medidas disciplinares executadas contra aqueles que violarem as normas da Vinland, ou cometerem qualquer tipo de infração corruptiva listada acima; e

(h) Prévia análise antes de contratação de terceiros.

Ademais, conforme mencionado acima, a Vinland não aceita em hipótese alguma a prática de qualquer das infrações objeto da Lei Anticorrupção, devendo os Colaboradores informar imediatamente ao Diretor de Compliance, Risco e PLD o conhecimento de qualquer atividade que se enseje na caracterização das infrações da Lei Anticorrupção.

Por fim, é considerada uma hipótese de desligamento imediato da Vinland, por justa causa, caso algum dos Colaboradores exerça algum ato de suborno ou de corrupção, conforme dispõe o subitem anterior e a Lei de Anticorrupção.

7. Política de certificação

A Vinland aderiu e está sujeita às disposições do Código ANBIMA de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

7.1. Atividades Elegíveis e Critérios de Identificação

Tendo em vista a atuação da Vinland como gestora de recursos de terceiros e distribuidora dos seus próprios fundos, a Vinland identificou, segundo o Código ANBIMA de Certificação, que a Certificação de Gestores ANBIMA ("CGA") e a certificação profissional ANBIMA série 20 ("CPA-20") são as únicas certificações descritas no Código ANBIMA de Certificação pertinentes às suas atividades, sendo a CGA aplicável aos profissionais da Vinland com alçada/poder discricionário de investimento e a CPA-20 aos que realizam a distribuição dos fundos de investimento diretamente junto a investidores, respectivamente.

Sem prejuízo do disposto acima, atualmente, a Vinland não realiza a atividade de distribuição de cotas dos fundos de investimento sob sua gestão, não sendo necessário que os Colaboradores detenham a certificação CPA-20, no entanto, tão logo a Vinland inicie tais atividades, se assegurará de que os Colaboradores que atuarem na distribuição dos fundos de investimento diretamente junto a investidores obtenham tal certificação.

Nesse sentido, a Vinland definiu que apenas o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor Responsável pela Administração de Carteiras de Valores Mobiliários, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA, ao passo que apenas o Colaborador com poder para realizar a distribuição dos fundos de investimento diretamente junto a investidores é elegível ao CPA-20.

Em complemento, a Vinland destaca que a CGA e a CPA-20 são pessoais e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pelo Diretor de Compliance, Risco e PLD.

Caso o Colaborador esteja exercendo a atividade elegível de CGA na Vinland, conforme acima indicada, e a certificação não esteja vencida a partir do vínculo do Colaborador com a Vinland, o prazo de validade da certificação CGA será indeterminado, enquanto perdurar o seu vínculo com a Vinland. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CGA na Vinland, a validade da certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível de CGA.

Com relação ao Colaborador certificado pela CPA-20 que se vincular a Vinland para exercer atividade elegível, conforme acima indicada, e desde que a sua certificação não esteja vencida na data do vínculo, terá o prazo de vencimento de sua certificação equivalente a 5 (cinco) anos, contados a partir da data da aprovação no exame ou da conclusão do procedimento de atualização, conforme o caso. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CPA-20 na Vinland, a validade da certificação será de até 3 (três) anos, contados da data de aprovação no exame ou da conclusão do procedimento de atualização, conforme o caso, ou, ainda, caso do Colaborador já ter atuado na atividade elegível anteriormente, o prazo será contado a partir da data de desligamento comunicada à ANBIMA, respeitado o prazo máximo de 5 (cinco) anos.

Desse modo, a Vinland assegurará que os Colaboradores que atuem nas atividades elegíveis participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos neste Manual e nos termos previstos no Código ANBIMA de Certificação.

Colaboradores certificados pela CPA-20 e que atuem em atividade elegível de CPA-20 na Vinland, deverão, para fins de atualização de sua certificação:

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

(i) participar de programa de treinamento oferecido pela ANBIMA com este propósito específico, desde que a conclusão do programa de treinamento e aprovação na avaliação final do curso ocorram até a data de vencimento da certificação, observado os prazos mínimos para realização dos cursos disponíveis no site da ANBIMA na internet; ou

(ii) participação em programas de treinamento, oferecidos ou validados pela Vinland, baseados no programa de atualização divulgado pela ANBIMA com este propósito específico, desde que a conclusão do programa de treinamento ocorra até a data do vencimento da certificação.

A atualização da certificação CPA-20, quando realizada por meio de programas de treinamento oferecidos pela Vinland, deve ser informada pela instituição no Banco de Dados da ANBIMA até o último dia do mês subsequente à data da conclusão do treinamento.

Colaboradores certificados pela CPA-20, mas que não atuem em atividade elegível de CPA-20 na Vinland, deverão, para fins de atualização de sua certificação, participar de programa de treinamento oferecido pela ANBIMA com este propósito específico, desde que a conclusão do programa de treinamento e aprovação na avaliação final do curso ocorram até a data de vencimento da certificação, observado os prazos mínimos para realização dos cursos disponíveis no site da ANBIMA na internet.

7.2. Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, o Diretor de Compliance, Risco e PLD deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados se o Colaborador possui alguma certificação ANBIMA, uma vez que, em caso positivo, a Vinland deverá inserir o Colaborador no Banco de Dados da Vinland.

Os Diretores Responsáveis pela Administração de Carteiras de Valores Mobiliários e pela Distribuição deverão esclarecer ao Diretor de Compliance, Risco e PLD se os Colaboradores que integrarão os departamentos técnicos terão ou não alçada/poder discricionário de decisão de investimento ou realizarão a distribuição dos fundos de investimento diretamente junto a investidores, conforme o caso.

Caso seja identificada a necessidade de certificação, o Diretor de Compliance, Risco e PLD deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

O Diretor de Compliance, Risco e PLD também deverá checar se colaboradores que estejam se desligando da Vinland estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à Vinland.

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer até o último dia útil do mês subsequente à data do evento que deu causa a atualização, nos termos do Artigo 12, §1º, I do Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Diretor de Compliance, Risco e PLD, conforme disposto abaixo.

7.3. Rotinas de Verificação

Semestralmente, o Diretor de Compliance, Risco e PLD, deverá verificar as informações contidas no Banco de Dados da ANBIMA, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos no Código ANBIMA de Certificação.

Ainda, o Diretor de Compliance, Risco e PLD deverá, semestralmente, contatar os Diretores Responsáveis pela Administração de Carteiras de Valores Mobiliários e pela Distribuição que deverão informá-lo se houve algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos e distribuição dos fundos, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso, bem como que possam realizar a distribuição dos fundos de investimento diretamente junto a investidores, se for o caso.

Colaboradores que não tenham CGA (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos do Artigo 17 do Código ANBIMA de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob gestão da Vinland sem a aprovação prévia do Diretor Responsável pela Administração de Carteiras de Valores Mobiliários, tendo em vista que não possuem alçada/poder final de decisão para tanto. Já os Colaboradores que não tenham CPA-20 estão impedidos de realizar a distribuição dos fundos de investimento diretamente junto a investidores.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pelo Diretor de Compliance, Risco e PLD, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor Responsável pela Administração de Carteiras de Valores Mobiliários por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente ou com a certificação vencida, o Diretor de Compliance, Risco e PLD deverá declarar, de imediato, o afastamento do Colaborador, devendo tal diretor, ainda, apurar as potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de adequação.

Sem prejuízo do disposto acima, anualmente deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento do Código de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

Por fim, serão objeto do treinamento anual de compliance assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da Vinland, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos e distribuição de cotas dos fundos sob gestão, reforçando que (a) somente os Colaboradores com CGA podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da Vinland, devendo os demais buscar aprovação junto ao Diretor Responsável pela Administração de Carteiras de

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

Valores Mobiliários e (b) somente os Colaboradores com CPA-20 poderão realizar a distribuição dos fundos de investimento diretamente junto a investidores; e; (iii) treinamento direcionado aos Colaboradores da Área de Compliance e Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

7.4. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do artigo 9º, §1ª, inciso V do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

Os profissionais já certificados, caso deixem de ser Colaboradores da Vinland, deverão assinar a documentação prevista no Anexo a este Manual denominado "Termo de Afastamento", comprovando o seu afastamento da Vinland. O mesmo procedimento de assinatura do Anexo aqui em referência, será aplicável, de forma imediata, aos profissionais não certificados ou em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

Este documento foi assinado eletronicamente por Ricardo José Sandoval Garcia Junior e ANDRE LAPORT RIBEIRO.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br:443 e utilize o código E49E-FF9A-109D-CC1A.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Certisign. Para verificar as assinaturas clique no link: https://www.portaldeassinaturas.com.br/Verificar/E49E-FF9A-109D-CC1A ou vá até o site https://www.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: E49E-FF9A-109D-CC1A

Hash do Documento

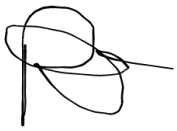
8C92AD6A8EED3385EB6CC37B417D1CF7D2EFE4808093F0D9D57D83F82B984B5D

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 04/04/2022 é(são) :

☑ RICARDO JOSÉ SANDOVAL GARCIA JUNIOR (Diretor de Compliance e Risco) - 218.021.858-36 em 28/03/2022 10:27 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Por email: ricardo.garcia@vinlandcap.com

Evidências

Client Timestamp Mon Mar 28 2022 10:27:14 GMT-0300 (Brasilia Standard Time)
Geolocation Latitude: -23.576576 Longitude: -46.6845696 Accuracy: 1235.6608797231847
IP 179.191.117.110
Assinatura:



Hash Evidências:
6BA1E3C68EB837A063EE19CB4D2FB0FB19BFDAEC6F1F12D9B4DC0AD8FDE62D6B

☑ André Laport Ribeiro (Diretor de Administração, Distribuição e Suitability) - 899.326.177-68 em 28/03/2022 10:11 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Por email: andre.laport@vinlandcap.com

Evidências

Client Timestamp Mon Mar 28 2022 10:11:06 GMT-0300 (Brasilia Standard Time)

Geolocation Location not shared by user.
IP 179.191.117.110
Assinatura:

Hash Evidências:
4233F1163BC9B3693D0A72433F30BD8852E5CB66DC5185D46A02AE28E7A26A78