POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CONTINUIDADE DE NEGÓCIOS

VINLAND Capital Management Gestora de Recursos Ltda.

VINLAND Capital Management International Gestora de Recursos Ltda.

VINLAND Capital Management Crédito Privado Gestora de Recursos Ltda.

Janeiro/2020

ÍNDICE

INTRODUÇÃO

A Política de Segurança da Informação e Continuidade de Negócios da Vinland ("Vinland"), é o 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.

OBJETIVOS

A presente política 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.

APLICAÇÕES DA POLÍTICA

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 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 e aos procedimentos e normas relacionadas, buscando orientação do Diretor de *Compliance* quando não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA POLÍTICA

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.

REQUISITOS DA POLÍTICA

O Diretor de *Compliance* 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.

Tanto a Política quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de *Compliance*.

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 ao Manual de Compliance da Vinland.

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*.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a gestora 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 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 acarretará violação às regras internas da empresa e sujeitará o usuário às sanções administrativas e legais cabíveis.

DAS RESPONSABILIDADES

1 - Da Gestão de Tecnologia e Segurança da Informação

O Diretor de *Compliance*, enquanto responsável pela presente Política de Segurança da Informação e Continuidade de Negócios, 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.
- 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* 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.
- 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 gestora 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 gestora 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 gestora.
- 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 gestora.

- 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);
    - 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, 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*;
- 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.

TESTES PERIODICOS DE SEGURANÇA EM SISTEMAS DE QUE CONTROLAM INFORMAÇOES 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 da 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.

A 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. Adicionalmente, a Vinland realiza testes anuais de contingência para validar o Plano de Continuidade de Negócios.

A efetividade da política de Confidencialidade e 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 e Riscos. 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 e Riscos 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;

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

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

São consideradas informações confidenciais para os fins deste Manual:

a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela VINLAND, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para o fundo de investimento gerido pela VINLAND, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da VINLAND e a seus sócios ou clientes, independente destas informações estarem contidas em pen-drives, hds, outros tipos de mídia ou em documentos físicos.

b) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na VINLAND, bem como informações estratégicas ou mercadológicas

e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da VINLAND e/ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela VINLAND ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Não são consideradas Informações Confidenciais, quaisquer informações que: (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador; (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao disposto neste Termo; (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade; (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade; (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente ao Diretor de Compliance da VINLAND para que as medidas legais cabíveis sejam tomadas

O Colaborador se compromete através do Termo assinado a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na VINLAND, comprometendo-se, portanto, observadas as disposições das Políticas da VINLAND, a não divulgar tais Informações Confidenciais para quaisquer fins ou pessoas estranhas VINLAND, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

O Colaborador se obriga a, durante a vigência deste Termo e por prazo

indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na VINLAND.

As obrigações ora assumidas ainda persistirão no caso do Colaborador ser transferido para qualquer subsidiária ou empresa coligada, afiliada, ou controlada pela VINLAND.

A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita a apuração de responsabilidades nas esferas cível e criminal.

O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a VINLAND e terceiros, ficando desde já o Colaborador obrigado a indenizar a VINLAND, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

O Colaborador reconhece e toma ciência que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na VINLAND são e permanecerão sendo propriedade exclusiva da VINLAND e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na VINLAND, devendo todos os documentos permanecer em poder e sob a custódia da

VINLAND, salvo se em virtude de interesses da VINLAND for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da VINLAND;

b) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à VINLAND todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da VINLAND, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

d) É expressamente proibida a instalação pelo Colaborador, de softwares não homologados pela VINLAND no equipamento do mesmo.

e) A senha que foi fornecida para acesso à rede de dados institucionais é pessoal e intransferível e não deverá, em nenhuma hipótese, ser revelada a outra pessoa.

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 gestora 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.

Serão geradas e mantidas trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantaremos controles de integridade para torná-las juridicamente válidas como evidências.

Serão implementados controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

Será monitorada toda 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);

Implementaremos 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;

A Vinland instalou sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CORREIO ELETRÔNICO

O objetivo desta norma é informar aos Colaboradores da Vinland quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da Vinland é para fins corporativos e relacionados às atividades do colaborador usuário dentro da empresa. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Vinland e também 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 gestora;
- 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 (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    - 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;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);
- 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);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
    - Nome do Colaborador
    - Departamento
    - Nome da empresa
    - Telefone (s)
    - Correio eletrônico

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 e Continuidade de Negócios.

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.

Como é do interesse da Vinland que seus Colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a

banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os Colaboradores que estão devidamente autorizados a falar em nome da Vinland para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os Colaboradores autorizados pela gestora 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.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa 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.

Os Colaboradores com acesso à internet poderão fazer o download (baixar) somente de programas ligados diretamente às suas atividades na Vinland e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo Diretor de *Compliance*.

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.

Os Colaboradores não poderão em hipótese alguma utilizar os recursos da Vinland para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a Vinland ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os Colaboradores não poderão utilizar os recursos da Vinland para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos.

Os serviços de comunicação instantânea (MSN, ICQ e afins) inicialmente não serão permitidos, mas poderão ser liberados caso o Diretor Responsável pela área solicitante requisite formalmente ao Diretor de *Compliance*.

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 (art. 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.

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* 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 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.

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 gestora, 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* da Vinland, ou de quem este determinar. As áreas que necessitarem fazer testes deverão solicitá-los previamente ao Diretor de *Compliance*, 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*.

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.
Documentos imprescindíveis para as atividades dos Colaboradores da empresa 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 e/ou detentores de contas privilegiadas 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*.

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

- Todos os computadores de uso individual deverão ter senha de Bios 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* 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 a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização do Diretor de *Compliance*.
- 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 Continuidade de Negócios e pelas normas específicas da gestora.
- 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.

DISPOSITIVOS MÓVEIS

A Vinland deseja facilitar a mobilidade e o fluxo de informação entre seus Colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da empresa, ou aprovado e permitido pelo Diretor de *Compliance*, como: notebooks, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A Vinland, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O Colaborador, portanto, 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 empresa.

Todo Colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

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* 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 empresa constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo Colaborador como: sua casa, hotéis, fornecedores e clientes.

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.

DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada semestralmente uma auditoria nos acessos ao Datacenter 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 Datacenter 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 Datacenter deverá ficar na posse do Diretor de *Compliance*, ou Colaborador definido por esta.

O Datacenter 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*.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero ou inflamável.

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

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

PLANO DE CONTINGÊNCIAS

De acordo com os requisitos da política, a presente seção tem o objetivo de estabelecer medidas a serem tomadas para identificar e prevenir contingências que possam causar

prejuízo para as atividades da Vinland. Nesse sentido, a Vinland entende que a prevenção e adequação de sua estrutura não são apenas necessárias, como primordiais de modo a prestar um ótimo serviço de gestão de recursos aos seus clientes.

Nessa inteligência, com o intuito de garantir a continuidade das atividades da Vinland, é feito o backup das informações digitais e dos sistemas existentes no escritório, através dos seguintes processos:

a) Backup diário realizado na nuvem;
b) Backup diário em disco externo as instalações físicas da Vinland;
c) Manutenção dos sistemas em funcionamento, apesar de falta de energia temporária, através de equipamentos de no break instalados para suprir o fornecimento de energia nos equipamentos principais para a manutenção das comunicações e atividades mínimas da Vinland;
d) Manutenção de um local externo, em um endereço fora das edificações e instalações físicas da Vinland, onde as atividades poderão ser mantidas no modelo de contingência;
e) Manutenção de meios remotos seguros para o trabalho de seus Colaboradores; e
f) Manutenção de servidor reserva.

1 Testes de Contingência

Os Testes de Contingência serão realizados com periodicidade mínima anual, de modo a permitir que a Vinland esteja sempre aprimorando sua infraestrutura para a continuação de suas atividades.

Os testes abrangerão os seguintes eventos, apenas de forma amostral, a saber:

a) Testes dos no-breaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;
b) Acesso aos sistemas e aos e-mails remotamente, do endereço externo;
c) Acesso aos dados armazenados externamente; e
d) Outros necessários à continuidade das atividades.

O resultado de cada teste será registrado no documento de Teste de Contingência.

SEGURANÇA CIBERNÉTICA

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

O acesso, uso indevido ou não autorizado dos ativos da VINLAND CAPITAL são tratados na Política de Segurança da Informação, parte integrante do Código de Ética.

A. Responsabilidades

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 a Diretoria de Compliance 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;

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

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 à diretoria;

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

Do responsável por Compliance

(i) Desenvolver, manter e implementar programas de treinamento e de conscientização aos Colaboradores Internos e Externos 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;

(iii) Emitir o Termo de Compromisso, conforme modelo do Código de Ética e Políticas Internas;

(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 Norma de Segurança da Informação e sugerir as alterações necessárias.

Equipamentos

Os equipamentos objeto desta Política são os de propriedade da VINLAND CAPITAL, tais como desktops, monitores, teclados, mouses, telefone, impressoras, desfragmentador de papéis e outros destinados ao uso pessoal ou comum dos Colaboradores da VINLAND CAPITAL. Eles deverão ser utilizados exclusivamente para fins profissionais, estão sujeitos à monitoramento pela Diretoria de Compliance e o uso indevido está sujeito às penalidades previstas no Código de Ética. 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 CAPITAL.

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.

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.

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

Senhas

A VINLAND CAPITAL 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 troca periódica de senhas pelos usuários ativos e cancela as senhas de usuários inativos/desligados da organização.

Softwares

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

Correspondências eletrônicas ("e-mails")

Apenas os Colaboradores Internos e sócios da VINLAND CAPITAL 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 Diretoria de Compliance.

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.

Os e-mails serão armazenados pela Microsoft, que proverá também os serviços de anti spam, anti vírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas.

Armazenamento de dados em nuvem

Para evitar a perda de informações proprietárias, confidenciais e/ou privilegiadas, a VINLAND CAPITAL adota a armazenagem automática de dados em nuvem.

Responsável: Adriano Moscheti – adriano.moscheti@vinlandcap.com – 11 3514 2528

Telefone

A VINLAND CAPITAL 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 CAPITAL 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, mediante acesso ao portal de telefonia contratado, a fim de fazer cumprir o Código de Ética.

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

Crises ou situações críticas

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

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.