POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

iVi Technologies

Versão 3

Novembro de 2023

Sumário

CONTROLE DE VERSÕES

Versão	Data Revisão	Revisor
1	Dezembro de 2021	Versão Inicial
2	Fevereiro de 2022	Lendel Augusto Vaz Lucas
3	Novembro de 2023	Lendel Augusto Vaz Lucas

1. Introdução

A Política de Segurança da Informação e Segurança Cibernética da iVi Capital aplica-se a todos os sócios, colaboradores, prestadores de serviços, incluindo trabalhos executados externamente ou remotamente por terceiros que utilizem o ambiente de sistemas de processamento da iVi, ou que acessem informações a esta pertencentes. Todo e qualquer usuário de recursos computadorizados, digitais ou sistêmicos da iVi tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos.

A Política de Segurança da Informação e Segurança Cibernética deve ser revisada e atualizada periodicamente, com o apoio das Áreas Administrativa e de Tecnologia, a fim de incorporar medidas relacionadas a atividades e riscos novos ou anteriormente não abordados. Caberá à Área de Compliance, por meio da aprovação das medidas apontadas pela área de Tecnologia, reeditar a Política de Segurança da Informação e Segurança Cibernética.

2. Objetivo

A Política de Segurança da Informação e Segurança Cibernética da iVi tem por objetivo permitir que a iVi Technologies cumpra com as exigências da autorregulação e regulamentação vigentes, manter o nível de segurança da organização em patamar definido como adequado pela iVi Technologies e proteger as informações de sua propriedade e/ou de terceiros que estejam sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade das mesmas.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da empresa, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais. Qualquer informação sobre a iVi Capital, ou de qualquer natureza relativa às atividades da empresa e a seus sócios, colaboradores e clientes só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Riscos e Compliance ou se permitido de qualquer forma pela presente política.

3. Aplicabilidade

Esta Política é aplicável a todos os Colaboradores da iVi Capital, independentemente do nível hierárquico, os quais deverão ter ciência de seu conteúdo e eventuais atualizações, e busca refletir:

- A estrutura adotada pela iVi para assegurar a proteção a informações confidenciais mantidas nos sistemas;
- Os critérios e os procedimentos básicos a serem adotados pelos Colaboradores da iVi a fim de minimizar o risco de exposição da informação confidencial;
- A periodicidade e o tipo de teste empregado a fim de verificar a integridade dos sistemas adotados.

A ciência pelos colaboradores das práticas, rotinas e procedimentos previstos nesta Política não os desobriga de ter conhecimento e de observar os conteúdos previstos nas demais políticas e manuais adotados pela iVi, incluindo, sem limitação, o Código de Ética e Conduta e o Manual de Controles Internos. Os Colaboradores que desejarem maiores informações sobre as políticas e manuais ou que tenham qualquer dúvida a respeito do conteúdo da presente Política e/ou dos procedimentos adotados, deverão contatar a equipe de compliance.

4. Segurança e Sigilo das Informações

Todos os Membros, enquanto estiverem trabalhando na iVi Technologies e mesmo após terem deixado a empresa, devem proteger a confidencialidade de quaisquer informações que não devam ser de domínio do público em geral, informações estas consideradas confidenciais, reservadas e/ou privilegiadas, obtidas durante o exercício de suas funções como Membros da iVi Technologies.

A iVi assegura que toda e qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem será previamente comunicada pelo Diretor de Riscos e Compliance. Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados possuem acesso seguro através de interfaces HTTPS bem como a autenticação segura e em ambientes segregados. Os acessos são controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada usuário colaborador ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

As medidas de segurança da informação utilizadas pela iVi Capital Management têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa e aos seus clientes.

São exemplos de informações que não deverão se tornar de domínio do público aquelas que digam respeito a:

I. Operações, estratégias, resultados, ativos, dados e projeções que sejam relevantes aos negócios da *iVi Technologies*;

II. Informações sobre o plano de negócios da *iVi Technologies*;

III. Informações confidenciais sobre os Membros da *iVi Technologies*;

IV. Informações sobre Clientes, distribuidores e fornecedores;

V. Qualquer informação considerada privilegiada.

5. Regras de acesso, proteção e controle:

I. Deve-se evitar manter nas mesas papéis e documentos confidenciais. É terminantemente proibido aos colaboradores a cópia ou impressão de arquivos utilizados, gerados ou disponíveis da iVi Capital para circulação em ambientes externos à empresa, sem a prévia e expressa autorização do Diretor de Riscos e Compliance. Isso ocorre, pois, tais arquivos podem conter informações consideradas confidenciais e/ou sensíveis aos objetivos sociais da gestora.

II. Em relação às informações de caráter sensível ou confidencial da empresa ou de clientes, estas serão armazenados em diretórios em nuvem, com backups e acesso restrito, e controlado pela equipe de Riscos e Compliance. Deve-se manter sigilo sobre senhas de acesso, do computador, rede e sistemas.

III. 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, responsabilizando-se também por seu extravio ou uso indevido.

IV. O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que

contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

V. Será obrigatória a alteração de senha de acesso (login de usuário) ao menos a cada 6 meses, utilizando modelo de definição de senha de difícil identificação por parte de potenciais "hackers" externos. Tal processo será auditável e rastreável eletronicamente pelo responsável pela TI, sob a supervisão do Diretor de Riscos e Compliance da iVi.

VI. A segregação das informações será feita através da ferramenta Google Drive. Membros somente terão acesso as suas pastas de trabalho, não conseguindo ter acesso a pastas de outros Membros. As diretorias terão acesso às pastas de trabalho de seus subordinados diretos e de seus departamentos. Dependendo da pasta, o acesso poderá ser em modo *"read only".* A Área de Compliance terá acesso a todas as pastas no modo *"read only"* para monitoramento.

VII. Os Membros têm acesso as suas pastas de maneira remota pelo sistema Google Drive podendo trabalhar, quando autorizados, de maneira remota.

VIII. As pastas de trabalho são pertencentes à função e não ao Membro. Caso um Membro mude de função dentro da instituição, seu acesso às pastas deve ser imediata e respectivamente alterado.

IX. O correio eletrônico (e-mail), ou qualquer outro meio de comunicação via internet, deve ser de uso preponderantemente profissional. É expressamente proibida a divulgação de mensagens com conteúdo religioso, racial, pornográfico ou político. Todos devem ser cautelosos no recebimento de e-mails de origem desconhecida, não abrindo arquivos ou links suspeitos.

X. Os colaboradores ou prestadores de serviços desligados da iVi Capital terão os seus acessos aos sistemas e programas de propriedade da Empresa ou adquiridos de terceiros imediatamente bloqueados após a comunicação de desligamento de tais colaboradores ou prestadores de serviços, de forma a preservar as informações confidenciais, reservadas ou privilegiadas.

XI. O acesso à área de trabalho deve ser feito somente por pessoal autorizado a acessar aquela área.

XII. Questões delicadas envolvendo assuntos da *iVi Technologies* não devem ser discutidas em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes etc. A utilização de celular em ambiente de trabalho também deve ser deixada para situações de emergência, isto é, quando não for possível a utilização dos telefones fixos da *iVi Technologies*.

XIII. É terminantemente proibido o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da iVi Capital, respondendo os responsáveis nos termos das políticas internas da iVi e da lei.

6. Organização dos Arquivos Eletrônicos

Os arquivos eletrônicos da *iVi Technologies* devem ser armazenados por um método homogêneo único e organizado que possibilite facilitar o acesso, a procura e consulta de documentos.

Os arquivos de trabalho devem ter nome que facilmente o identifique, devem conter os dados que sejam relevantes quando um Membro for procurá-lo. O nome deve ser objetivo, intuitivo e direto. Os arquivos cuja sua data seja relevante, devem conte-la no início do nome. Arquivos cujo assunto for essencial, deve conter também no nome.

A árvore de pastas onde os arquivos serão armazenados devem estar organizadas e nomeadas de maneira lógica e intuitiva, que permita ao Membro autorizado facilmente encontrar o arquivo procurado.

A Área de Compliance deve ditar as diretrizes de armazenamento de dados. As árvores de pastas e nomenclaturas de arquivos de cada Membro devem ser aprovadas pela Área de Compliance, estando estes sujeitos a seguir as mudanças exigidas pela Área de Compliance sempre que necessário.

É de responsabilidade de cada Membro armazenar e manter seus arquivos organizados, seguindo as diretrizes da Área de *Compliance*. Infringir as diretrizes pode gerar penalidades ao Membro.

7. Segurança de Dispositivos e Equipamentos

I. Proteção contra vírus: para proteção contra vírus deverão ser instalados softwares de prevenção nos servidores de rede da *iVi Technologies*. Além disso, semestralmente, serão verificados todos os hard-disks de todos os computadores.

II. Segurança dos Arquivos: Diariamente serão realizados backups de todos os arquivos de dados salvos na rede (base de dados, planilhas, textos, etc.). Estes backups serão realizados na plataforma do Google Drive, ou em qualquer outra plataforma aprovada pelo Gestor de Tecnologia.

III. Segurança do Hardware: Os equipamentos devem ser instalados em locais adequados, protegidos de raios solares, altas temperaturas e de incidência de poeira. Além das providências acima, podem ser instalados nobreaks, devidamente dimensionados, para garantir:

a) A uniformidade da tensão da rede, em casos de picos de energia;
b) No mínimo, o salvamento de dados e o desligamento apropriado dos equipamentos, nas faltas de energia elétrica.

8. Informações a Clientes e ao Público em Geral

De maneira geral, informações sobre a *iVi Technologies* e seus produtos deverão somente ser pronunciadas por pessoas devidamente designadas pela diretoria. Os demais Membros devem evitar quaisquer declarações, orais ou por escrito, que represente de maneira equivocada:

I. Os serviços que Membros e a *iVi Technologies* são capazes de realizar;
II. Qualificações dos Membros ou da *iVi Technologies*; e
III. Credenciais profissionais ou acadêmicas dos Membros.

8.1 Publicidade

A *iVi Technologies* se utiliza das Diretrizes para Publicação e Divulgação de Material Técnico para Fundos de Investimento da ANBIMA como base para publicidade de seus produtos.

O conceito de publicidade, de acordo com as diretrizes da ANBIMA, abrange toda forma de comunicação, entre a *iVi Technologies* e os investidores (cotistas) ou potenciais investidores – de forma impessoal e indiscriminada – e que seja fruto de uma estratégia mercadológica. São exemplos de publicidade, mas não a estes limitados: quaisquer materiais publicados ou elaborados para uso em mídia pública (jornal, revista, internet e similares) ou disponibilizados para o público em geral (agência, outros locais públicos, mala direta ou demais materiais para destinatários que não sejam de relacionamento da instituição), notadamente com objetivo comercial e fruto de estratégia mercadológica.

Toda publicidade emitida em nome da *iVi Technologies* deve estar não só em concordância com as regulamentações existentes, mas também zelar para divulgar da forma mais adequada possível a marca *iVi Technologies*.

Qualquer material de divulgação deverá ser previamente aprovado pela Área de Compliance da *iVi Technologies*.

8.2 Relacionamento com a imprensa

Da mesma forma, o relacionamento com a imprensa deve ser pautado no compromisso de fornecer informações precisas e transparentes, de forma a manter uma relação de confiança com os meios jornalísticos e a boa imagem da empresa perante o público em geral.

Todo material de imprensa escrita (notas de jornais, artigos de revistas, contribuição para blogs/sites de notícias, e-mails ou cartas (mala direta) a Clientes e outros sistemas de informação escrita) deverá ser previamente revisado e expressamente aprovado pela Área de Compliance da *iVi Technologies*, antes da sua divulgação.

As declarações dos Membros perante quaisquer órgãos de imprensa deverão ter seu conteúdo previamente discutido e aprovado pela Área de Compliance com o objetivo de alinhar as exposições às estratégias e filosofia da *iVi Technologies*. Somente pessoas previamente autorizadas pela diretoria poderão falar em nome dos produtos e da *iVi Technologies*.

9. Ocorrências de Curso Anormal

Diante de incidentes, a iVi atua no mapeamento das atividades consideradas críticas e essenciais para a continuidade dos negócios. O registro, a análise da causa e do impacto,

bem como o controle dos efeitos de incidentes relevantes, caso ocorram, deverão ser registrados e controlados por formulário específico contendo as informações abaixo:

- Data de Ocorrência;
- Breve Relato;
- Consequências;
- Providências para regularização;
- Ciência e despacho da Diretoria;
- Evidências.

Por meio das ocorrências registradas no referido formulário, os profissionais da área de tecnologia da informação atuam no sentido de mitigar e evitar reincidência e/ou novos incidentes.

Para a prevenção e tratamento dos incidentes a serem adotados por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou relevantes, a iVi adota o envio de um termo de confidencialidade das informações que deverá ser lido, compreendido e assinado por todos os prestadores de serviços.

Para a classificar os dados e as informações quanto à sua relevância são considerados:

- Nível de importância das informações;
- Grau de confidencialidade;
- Conteúdo, quando confidencial, estratégico ou que envolve dados cadastrais;
- Classificação do profissional responsável pela atividade;
- Classificação da área/departamento;
- Atividades que exigirá o uso da informação.

Os parâmetros abaixo são os utilizados na avaliação da relevância dos incidentes:

- A classificação da criticidade do recurso afetado;
- A classificação da criticidade da informação;
- O tempo de resposta, restauração e regularização do incidente;
- Os tipos de contornos, ou seja, qual o procedimento a ser realizado interinamente até a regularização do incidente.

10. Identificação de Suspeitas

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou

ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance prontamente. O Diretor de Compliance determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras, deverão ser notificados. Ademais, o Diretor de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação e quais medidas deverão ser tomadas. Caso necessário, o Diretor de Compliance notificará, em prazo compatível com a severidade do evento, a Autoridade Nacional de Proteção de Dados.

11. Testes Periódicos de Segurança

A fim de verificar a integridade dos sistemas adotados, inclusive com relação aos sistemas de informações confidenciais mantidas em meio eletrônico, a equipe de tecnologia da informação realiza testes semestrais, formalizados por meio de relatório enviado ao Diretor de Compliance e Riscos. Semestralmente a equipe de tecnologia da informação enviará e-mails separados para os respectivos coordenadores de cada Colaborador, contendo a lista de todos os sistemas e quais Colaboradores possuem acesso a cada um. Os coordenadores deverão confirmar as prerrogativas dos Colaboradores e se deverá ser mantido o acesso a cada um desses sistemas. Em linha com o exposto acima, o relatório semestral a ser enviado ao Diretor de Compliance e Riscos deverá conter:

- A lista de todos os sistemas e quais Colaboradores possuem acesso a cada um, preparada em linha com as confirmações dos respectivos coordenadores;
- Informações do prestador de serviços de sistemas, somente caso ocorra algum incidente envolvendo-o;
- Eventuais inconsistências detectadas em cada um dos sistemas.

O Diretor de Compliance e Riscos deverá revisar a lista de atribuições, confirmando a adequação dos acessos de cada Colaborador ao seus respectivos cargos e prerrogativas, além de adotar eventuais medidas cabíveis para correção das inconsistências detectadas no relatório descrito acima e nas melhorias contínuas dos procedimentos relacionados com a segurança cibernética registradas nesta política.