IG4 CAPITAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
IG4 CAPITAL INVESTIMENTOS LTDA.
("Gestora")

Versão vigente: janeiro/2025
Versão anterior: junho/2022

Aprovada por: _____

Signed by:
Ivan Apsan
32AA0CF572734B1...

Ivan Apsan Frediani

Diretor de Compliance

CAPÍTULO I
DO OBJETIVO

1.1. O presente instrumento tem por objetivo formalizar a Política de Segurança da Informação ("Política") adotada pela IG4 Capital, com caráter permanente, a fim de apresentar e disseminar entre os Colaboradores os procedimentos de controle utilizados para garantir a segurança das informações produzidas e gerenciadas dentro do ambiente de trabalho.

1.2. Deste modo, é responsabilidade de todos os Colaboradores garantir a confidencialidade e integridade das informações produzidas durante a execução do trabalho na Gestora, sendo fundamental que todos os Colaboradores tenham plena consciência a respeito da importância de cada um na garantia da efetividade dos procedimentos definidos nesta política.

1.3. É exigido também o comprometimento no cumprimento desta Política por todos os Colaboradores da IG4 Capital.

1.4. Qualquer colaborador que tiver conhecimento a respeito do descumprimento da presente política deverá comunicar ao Departamento de Compliance, por meio do e-mail compliance@ig4capital.com ou efetuar um relato por meio do Canal de Denúncias da Gestora.

CAPÍTULO II
DA ABRANGÊNCIA

2.1. Entende-se por "colaboradores", em linha com o conceito definido pelo Código de Ética e Conduta da Gestora: (i) sócios e associados; (ii) funcionários; (iii) diretores; (iv) estagiários; ou (v) quaisquer pessoas que, em virtude de seus cargos, funções ou

posições na Gestora, tenham acesso à informação gerada internamente e/ou recebida de clientes para o desenvolvimento de trabalhos internos.

2.2. Todos os Colaboradores devem ter ciência de que toda a informação gerada internamente ou recebida é estritamente confidencial. A responsabilidade de confidencialidade e integridade das informações terá validade mesmo após o desligamento do Colaborador, sendo que o não cumprimento das disposições previstas nesta Política será consideração com infração grave, passível de sanções administrativas e/ou judiciais.

CAPÍTULO III
DAS DIRETRIZES E PROCEDIMENTOS

3.1. Controle de Acesso:

A troca de informações entre os Colaboradores da Gestora deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida, o Departamento de Compliance deverá ser acionado previamente à revelação.

De forma a assegurar o controle de Informações Confidenciais, as seguintes medidas são utilizadas:

(i) login e senha para acesso à rede de computadores individuais para cada Colaborador, bem como para acesso a e-mail e dispositivos móveis de uso profissional, sendo tal senhas pessoais e intransferíveis;

(ii) proibição de conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de tecnologia da Gestora, não sendo permitido que os Colaboradores utilizem computadores, discos externos ou quaisquer outros dispositivos não relacionados ao desempenho de suas atividades.

(iii) rede de informações eletrônicas com a utilização de servidores exclusivos da Gestora, evitando acessos de terceiros;

(iv) manutenção de diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos Colaboradores, com registro de acesso a tais pastas e arquivos por parte dos Colaboradores com base na senha e login de cada Colaborador, e proteção contra adulterações e manutenção de registros que permitam auditorias e inspeções;

(v) monitoramento de acesso a sites, blogs, fotologs e webmails, entre outros, bem como os e-mails enviados e recebidos;

(vi) monitoramento, inclusive por meio de gravações, de ligações telefônicas realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela IG4 Capital para a atividade profissional de cada Colaborador; e

(vii) bloqueio de acesso aos sistemas pelo departamento de TI, sempre que solicitado pelo Departamento de Compliance, ou caso seja detectado pelo departamento de TI algum risco para a rede ou os sistemas da Gestora.

O Colaborador poderá ser responsabilizado caso disponibilize quaisquer de suas senhas a terceiros.

O departamento de tecnologia da informação ("TI") fará verificações semestrais na rede corporativa da Gestora, para validar o acesso seguro aos recursos disponíveis, bom uso de equipamentos e informações comuns a mais de um setor da Gestora, preservação de Informações Confidenciais e identificação das pessoas que tiveram ou tenham acesso a estas, proteção contra adulterações e manutenção de registros que permitam auditorias e inspeções. Ao final de cada verificação será encaminhado um e-mail pela Área de TI para o Departamento de Compliance reportando a conclusão dos exames realizados, inclusive eventuais irregularidades ou falhas verificadas.

Em relação às vias físicas, documentos contendo Informações Confidenciais devem ser objeto de arquivo com acesso restrito e devem ser triturados previamente ao seu descarte, evitando acesso indevido a tais informações, observada as normas relativas à conservação de documentos pelos períodos legais aplicáveis.

A sede da Gestora possui segregação física de espaços, de forma que (i) acesso ao espaço alocado ao Compliance seja restrito aos respectivos Colaboradores; (ii) reuniões, inclusive com não colaboradores, sejam realizadas de forma reservada, em salas específicas e segregadas do espaço alocado à atividade de gestão.

3.2. Backup:

Todos os documentos arquivados nos computadores da Gestora são objeto de backup diário na nuvem com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

3.3. Cópia de arquivos e instalações:

Todos os programas de computador utilizados pelos Colaboradores devem ter sido previamente autorizados pelo responsável pela Área de TI. Downloads de qualquer

natureza podem ser realizados, desde que de forma justificada.

A cópia de arquivos e instalação de programas em computadores da Gestora deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. Nestes casos, o Colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Gestora. É vedada, ainda, a manutenção destes em mesas, máquinas de fax ou copiadoras.

3.4. Descarte de Informações:

O descarte de informações confidenciais deve observar as seguintes diretrizes:

(i) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;

(ii) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;

(iii) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada.

(iv) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Gestora devem ser apagados de modo que a informação protegida que havia neles seja irrecuperável.

3.5. Redundância:

Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe poderá acessar as informações na nuvem de qualquer local.

Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho e o servidor estão conectados a um equipamento do tipo no-break, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuários salvem seus arquivos.

3.6. Suporte e Monitoramento:

Em caso de pane da rede ou em alguma estação de trabalho, o fato deverá ser imediatamente comunicado à Área de TI, que assegurará o suporte interno ou providenciará que seja acionado o suporte externo necessário.

Os sistemas eletrônicos utilizados pela Gestora estão sujeitos à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

Nesse sentido, tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos Colaboradores.

Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve ser objeto de informação ao Compliance para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

3.7. Tratamento de casos de vazamento de informações confidenciais:

No caso de vazamento de informações confidenciais relacionadas a investidores, ou de qualquer outro Dado Pessoal ou Dado Pessoal Sensível tratado pela Gestora (regra de Tratamento de Dados a seguir), ainda que oriundo de ação involuntária, o Diretor de Compliance notificará os interessados sobre o ocorrido. Em se tratando de Dado Pessoal ou Dado Pessoal Sensível, a Autoridade Nacional de Proteção de Dados também deverá ser comunicada, além do titular do dado. Esta comunicação observará os parâmetros exigidos pela Lei Geral de Proteção de Dados.

Sem prejuízo, a Gestora acionará o seu Plano de Recuperação visando a identificação da

causa que ensejou o vazamento e responsabilização do causador. Ademais, será elaborado um Relatório acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

Este Relatório será elaborado pelo Diretor de Compliance e será submetido à Diretoria da Gestora que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

3.8. Firewall:

A Gestora faz o uso da tecnologia de Firewall para proteger sua rede contra ameaças externas.

3.9. Testes de Segurança:

São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

Teste	**Periodicidade**
Controle de dispositivos conectados	Por demanda
Controle de acesso	Anual
Testes de dupla autenticação	Mensal

CAPÍTULO IV
TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS

4.1. A Gestora zela pela observância, implementação e cumprimento de regras, políticas e procedimentos relacionados à Segurança da Informação.

4.2. Sem prejuízo das diretrizes contidas na Política de Segurança da Informação acima e com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, a Gestora adota regras e procedimentos para o tratamento de dados pessoais e, eventualmente, dados sensíveis, inclusive nos meios digitais, em linha com a Lei Geral de Proteção de Dados.

4.3. A maneira como a IG4 Capital utiliza os dados pessoais e realiza o seu tratamento está definida na Política de Privacidade de Dados, disponível no website para consulta e com o Departamento de Compliance.

4.8. A Gestora é responsável por garantir a segurança dos dados tratados, sem prejuízo do treinamento dos Colaboradores com relação à matéria.

CAPÍTULO V
DAS DISPOSIÇÕES GERAIS

5.1. A Interpretação desta Política deve ser executada por todos os Colaboradores, em conjuntos com as normas e procedimentos que estão previstos no Código de Ética e Conduta da IG4 Capital Investimentos Ltda. e, quando necessário, em consulta ao Departamento de Compliance da Gestora.

5.2. Qualquer infração ou suspeita de infração desta Política deverá ser comunicada ao Departamento de Compliance, por meio do Canal de Denúncias da IG4 Capital (https://ig4capital.becompliance.com/compliance/canal-denuncias) ou pelo e-mail compliance@ig4capital.com e deverá ser tratada nos termos e penalidades impostas pela Gestora.