POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA
B5 INVESTIMENTOS CONSULTORIA DE VALORES MOBILIÁRIOS LTDA.

1. OBJETIVO

Esta política tem por objetivo estabelecer diretrizes que permitam a todos os colaboradores, parceiros, fornecedores e clientes da B5 INVESTIMENTOS CONSULTORIA DE VALORES MOBILIÁRIOS LTDA. ("Consultoria"), seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Para tal, destacamos os seguintes pontos na política:

a) Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.
b) Ofertar a todos os colaboradores orientações sobre a utilização dos recursos computacionais, de Telecomunicação e infraestrutura de TI;
c) Garantir que a informação seja mantida em seu estado original, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais. (Integridade).
d) Garantir que o acesso à informação seja obtido somente por pessoas autorizadas. (Confidencialidade).
e) Garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. (Disponibilidade).

2. ABRANGÊNCIA

Esta política se aplica a todos os sócios, diretores, colaboradores, parceiros, estagiários e prestadores de serviço que tenham algum vínculo com a Consultoria ("Integrantes"), que, direta ou indiretamente, utilizam ou suportam os sistemas, infraestrutura ou informações da empresa. Todos esses serão tratados nesta política como usuários.

3. DIRETRIZES PARA O USO DE EQUIPAMENTOS ELETRÔNICOS

3.1 Os usuários devem utilizar preferencialmente os equipamentos eletrônicos de propriedade da organização para as atividades profissionais.

3.2 A utilização de equipamentos particulares em rede interna fica condicionada ao cumprimento dos requisitos de segurança.

3.3 Na hipótese de dúvidas e/ou problemas relacionados aos equipamentos, sistemas ou softwares internos, os usuários devem imediatamente comunicar a administração. Caso não realize a imediata comunicação, o usuário poderá ser

responsabilizado por eventuais ocorrências que poderiam ser evitadas com a prévia comunicação.

4. RESPONSABILIDADES

4.1 Das Responsabilidades específicas dos Integrantes

Será de inteira responsabilidade de cada integrante, o prejuízo ou dano que vier a sofrer ou causar à Consultoria e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas. Na hipótese de ocorrer qualquer dano decorrente do mau uso ou negligência, as despesas para a recuperação do equipamento serão suportadas pelo usuário.

Ter postura exemplar em relação à segurança da informação, realizar backups periódicos dentro da infraestrutura disponível, não compartilhar senhas, não disseminar notícias ou informações inconsistentes.

4.2 São responsabilidades da Consultoria e/ou processos:

a) Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento desta e das demais Políticas da Consultoria
b) Exigir dos colaboradores a assinatura do Termo de confidencialidade, o seguimento das normas estabelecidas, bem como o comprometimento de manter sigilo e confidencialidade, sobre todos os ativos de informações da Consultoria

5. MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política, a Consultoria poderá:

a) Implantar sistemas de monitoramento nas estações de trabalho, plataformas parceiras, 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;
b) Fornecer as informações obtidas pelos sistemas de monitoramento e auditoria às autoridades competentes, em caso de exigência legal, regulatória ou judicial, observada a Lei nº 13.709/2018;

c) realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
d) instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

A Consultoria registra os acessos aos seus sistemas e assegura a realização de testes periódicos de segurança dos sistemas de informação, em especial dos mantidos em meio eletrônico, na forma do art. 19, § 1º, VI, da Resolução CVM nº 19/21. Os registros são protegidos contra adulteração e conservados pelo prazo mínimo de 5 (cinco) anos.

6. UTILIZAÇÃO DOS SERVIÇOS DE CORREIO ELETRÔNICO CORPORATIVO

O objetivo desta Política é informar aos Integrantes quais são as atividades permitidas e proibidas quanto ao uso do serviço de email corporativo.

Acrescentamos que é proibido aos Integrantes o uso do correio eletrônico da Consultoria para:

a) Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Consultoria;
b) 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;
c) Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a vulneráveis a ações civis ou criminais;
d) Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
e) Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
f) Produzir, transmitir ou divulgar mensagem que contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Consultoria;
g) Contenha ameaças eletrônicas, como: spam, phishing, vírus de computador;
h) 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;
i) Vise obter acesso não autorizado a outro computador, servidor, sistema ou dispositivo da rede;

j) Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
k) Vise burlar qualquer sistema de segurança;
l) Vise vigiar secretamente ou assediar outro usuário;
m) Vise acessar informações confidenciais sem explícita autorização do proprietário;
n) Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
o) Inclua imagens criptografadas ou de qualquer forma mascaradas;
p) Contenha anexo(s) superior(es) a 20 MB para envio (interno e internet) e 20 MB para recebimento (internet);
q) Tenha conteúdo considerado impróprio, obsceno ou ilegal;
r) Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
s) Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
t) Tenha fins políticos locais ou do país (propaganda política);
u) Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

7. UTILIZAÇÃO DO SERVIÇO DE INTERNET

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

a) 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, email, 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;
b) A Consultoria, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer integrante, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao integrante. 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 instituição cooperará ativamente com as autoridades competentes;

c) Como é do interesse da Consultoria que seus Integrantes 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;
d) Somente os colaboradores que estão devidamente autorizados a falar em nome da Consultoria para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros;
e) Apenas os colaboradores autorizados pela instituição 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;
f) É proibida a divulgação e/ou o compartilhamento indevido de informações das áreas da Consultoria 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;
g) 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 Consultoria
h) Os colaboradores não poderão em hipótese alguma utilizar os recursos da Consultoria para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
i) Materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
j) O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming e comunicadores instantâneos (rádios on-line, canais de broadcast, Whatsapp, X e afins) estão permitidos;
k) Não é permitido acesso a sites de proxy.

8. IDENTIFICAÇÃO DO INTEGRANTE

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

8.2. O uso dos dispositivos e/ou senhas de identificação de outra pessoa pode configurar ilícito civil e penal, inclusive o crime de falsa identidade (art. 307 do Código Penal).

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

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

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

8.6. É proibido o compartilhamento de login para funções de administração de sistemas, bem como a troca de equipamentos entre os usuários sem a devida autorização.

8.7. 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.

8.8. 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.

8.9. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou acionar à área técnica responsável para cadastrar uma nova.

8.10. Casos omissos a este tópico deverão ser considerados com base no processo mais restritivo.

9. COMPUTADORES, DISPOSITIVOS MÓVEIS E RECURSOS TECNOLÓGICOS

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

9.2. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos serão realizadas via pelos analistas técnicos de tecnologia, após sua disponibilização pelo fabricante ou fornecedor.

9.3. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Consultoria

a) Tentar ou obter acesso não autorizado a outro computador, servidor, sistema ou rede;
b) Burlar quaisquer sistemas de segurança;
c) Acessar informações confidenciais sem explícita autorização do proprietário;
d) Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
e) Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
f) Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
g) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
h) Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

9.4. Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, como: notebooks, smartphones, HDs externos e pendrives.

9.5. 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.

9.6. A Consultoria, 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.

9.7. 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, mesmo depois de terminado o vínculo contratual mantido com a Consultoria

9.8. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados.

9.9. 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.

9.10. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Consultoria, notificar imediatamente os diretores da Consultoria Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

9.11. O integrante deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos.

9.12. Os dispositivos móveis que contenham informações confidenciais devem possuir criptografia.

10. CLASSIFICAÇÃO DA INFORMAÇÃO

10.1. A classificação da informação é um processo essencial para a segurança, gerenciamento e proteção de dados na Consultoria

10.2. Posto isto, Informações sensíveis ou confidenciais, como dados pessoais, estratégicos ou financeiros, precisam ser tratados com rigor em termos de proteção, garantindo que tais dados sejam armazenados, processados e transmitidos de forma segura, minimizando os riscos de vazamento, perda ou ataques cibernéticos, em observância à Lei Geral de Proteção de Dados (Lei Nº 13.709, de 14 de Agosto de 2018).

10.3. As informações dos clientes, as recomendações, as estratégias e os dados internos da Consultoria são confidenciais. É vedado ao Integrante utilizar, revelar ou transferir essas informações a pessoas não autorizadas ou que possam vir a utilizá-las indevidamente, durante e após o vínculo com a Consultoria.

10.4. Os incidentes de segurança da informação são registrados e analisados, e a Consultoria mantém plano de resposta a incidentes e programa anual de

conscientização dos Integrantes. O incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais é comunicado à Autoridade Nacional de Proteção de Dados e aos titulares afetados, na forma do art. 48 da Lei nº 13.709/2018 e da Resolução CD/ANPD nº 15/2024, no prazo de 3 (três) dias úteis contado do conhecimento do incidente.

11. PENALIDADES

11.1. Caso seja constatada a inobservância das diretrizes ou a verificação da ocorrência de qualquer prática vedada da presente Política ("infrações"), serão aplicadas penalidades conforme a gravidade do fato.

11.2. As suspeitas de infração da Política passarão por processo criterioso de análise pelos setores responsáveis**.**

11.3. O descumprimento desta Política sujeita o Integrante às medidas disciplinares previstas nos instrumentos que regem a sua relação com a Consultoria, entre elas o desligamento ou a rescisão do vínculo, conforme a gravidade e a reincidência, sem prejuízo das sanções legais e regulatórias aplicáveis. Cumulativamente, a Consultoria poderá recolher o equipamento disponibilizado pela organização e cobrar todos os valores necessários para a reparação dos danos causados.

11.4. O Integrante será responsável pela manutenção zelosa dos equipamentos de propriedade da Consultoria Eventual dano, extravio e/ou perda total do equipamento que estiver sob sua posse implicará a integral e irrestrita responsabilização pelos prejuízos pecuniários causados a organização e/ou terceiros, conforme Contrato de Comodato assinado individualmente por cada usuário.

11.5. Na hipótese de a infração implicar em danos a terceiros, o usuário será individualmente responsabilizado por todas as despesas e custos para a reparação do dano alegado.

12. VALIDADE DO DOCUMENTO

12.1. A presente Política é disponibilizada de forma clara, acessível e atualizada para todos os seus colaboradores.

12.2. Este documento é válido por prazo indeterminado, a partir da data de sua aprovação, e poderá ser alterado a qualquer momento, sem aviso prévio, caso ocorram circunstâncias que exijam tal mudança.

12.3. A área de Compliance será responsável por informar aos Integrantes sobre qualquer atualização ou nova versão desta política e disponibilizará o documento.

12.4. A versão mais recente da política revoga todas as versões anteriores e entrará em vigor a partir da data de sua aprovação.

Atualizado em: setembro de 2026.