DSK CAPITAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

I. Histórico de Modificações do Documento

Data	Responsável	Versão	Alterações/Inclusões
Julho/2021	Diretor de Compliance e Riscos	001	Criação da Política
Março/2023	Diretor de Compliance e Riscos	002	Atualização do Código

A Política de Segurança Cibernética e da Informação ("Política") tem caráter permanente. O conteúdo deste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes, mediante aprovação da maioria dos sócios da DSK Capital. Os profissionais da DSK Capital e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível. Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

II. Termos Gerais

A Política de Segurança Cibernética e da Informação da DSK Capital visa estabelecer regras de uso dos ativos e dos recursos da DSK Capital com o objetivo de minimizar riscos operacionais e estabelecer padrões de utilização das informações pertencentes à DSK Capital, além de mitigar os riscos de uma ameaça cibernética por meio da implementação de um programa de segurança cibernética.

A Política aplica-se a todos os níveis hierárquicos da DSK Capital: sócios, dirigentes, empregados, consultores, funcionários, trainees, estagiários e prestadores de serviços ("Colaboradores") e todos os Colaboradores estão cientes de que devem conhecer e respeitar todas as normas aqui dispostas e que o descumprimento de tais normas poderá acarretar a imposição pelo Diretor de Compliance e Riscos das seguintes sanções administrativas a depender do grau de gravidade da conduta: (i) assinatura de termo de compromisso; (ii) advertência escrita ou verbal; (iii) censura; (iv) suspensão; ou (v) demissão/término da relação contratual.

A DSK Capital estabelece que é responsabilidade de cada um de seus Colaboradores garantir a total confidencialidade e integridade das informações diariamente produzidas em razão de e/ou no ambiente de trabalho, sendo essencial que todo Colaborador tenha plena consciência acerca de sua importância no processo de garantia do cumprimento dos procedimentos definidos por meio desta Política.

Todos os Colaboradores estão cientes de que toda informação gerada internamente pela DSK Capital e/ou recebida de clientes para o desenvolvimento de trabalhos de qualquer natureza é estritamente confidencial e deve manter-se íntegra durante toda a sua existência. Além disso, os Colaboradores, ao utilizarem qualquer meio eletrônico (chats, Skype, e-mails, internet, entre outros) para o desenvolvimento de suas atividades, devem considerar seu uso como ferramenta de trabalho e, como tanto, de propriedade da empresa para uso profissional e de interesse da organização. A utilização de meios eletrônicos para fins particulares é terminantemente proibida. Vale salientar, ainda, que os acessos a e-mails e à internet, assim entendidos como ferramentas de trabalho de propriedade da DSK Capital, passam por backups diários e poderão ser objeto de auditorias e revisões a qualquer momento, estando à total disposição da administração da empresa.

A responsabilidade do Colaborador e/ou prestador de serviços em questão de confidencialidade e integridade das informações é válida até mesmo após o seu desligamento e deve ser cumprida de acordo com os itens desta política.

Ciente de que o acesso a informações pessoais recebidas por cada um de seus Colaboradores não pode ser coibido, a DSK Capital cordialmente solicita o não fornecimento de endereços eletrônicos profissionais para

fins pessoais. Adicionalmente, a DSK Capital recomenda prudência e cautela para a abertura de arquivos anexos a mensagens eletrônicas e páginas da internet, em especial no que tange a conteúdo inapropriado. O acesso a conteúdo não condizente com o ambiente de trabalho será alvo de investigação e, caso constatado, estará sujeito às sanções cabíveis.

Com o objetivo de garantir maior alinhamento da conduta de todos os seus Colaboradores, este documento abordará alguns itens de maneira direta e específica. Vale salientar, entretanto, que esta Política não deve se restringir aos aspectos tratados a seguir e que eventuais dúvidas e/ou questionamentos devem ser imediatamente levados ao conhecimento do Diretor de Compliance e Riscos da DSK Capital.

III. Infraestrutura

A DSK Capital disponibiliza a seus Colaboradores infraestrutura composta por hardwares e softwares necessários ao desenvolvimento de suas atividades A fim de garantir a segurança das informações processadas, a DSK adota, dentre outras, as seguintes medidas:

- Todo equipamento possui um programa firewall de segurança para acesso a sua rede;
- Cada equipamento possui um programa antivírus para manter o ambiente livre de ameaças e acessos mal-intencionados;
- Existem dois provedores de acesso à internet, e-mail e telefonia para aumentar a confiabilidade e disponibilidade de acesso aos colaboradores;
- Para acesso remoto, os Colaboradores estão cientes de que devem utilizar apenas rede wi-fi privada, com proteção por senha, e manter o *firmware* do roteador sempre atualizado, trocando o roteador caso verificados riscos de privacidade;

IV. Controle de Acesso

Para acesso às estações de trabalho, correios eletrônicos (e-mails), softwares e demais dispositivos é obrigatório o uso de senhas e cabe a cada Colaborador a responsabilidade por manter a confidencialidade e segurança de suas credenciais de acesso. As senhas deverão possuir validade máxima de 1 (um) ano e podem ser substituídas a qualquer momento por decisão do Diretor de Compliance e Riscos ou por solicitação formal do Colaborador.

A DSK Capital poderá monitorar a utilização de computadores, telefones, internet, e-mail e demais aparelhos, visto que tais recurso se destinam exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores. Nesse sentido, a DSK Capital:

- Manterá diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos colaboradores e, com base na senha e login disponibilizados, irá monitorar o acesso dos colaboradores a tais pastas;
- Poderá monitorar o acesso dos colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos, sendo certo que a internet (i) não poderá ser utilizada como ferramenta para download ou distribuição de software ou dados não legalizados; e (ii) não deve ser utilizada como ferramenta para divulgação de informações confidenciais em grupos de discussão, instant Messenger ou outros meios de comunicação;
- Poderá, a seu exclusivo critério, bloquear o acesso a determinados arquivos ou domínios;
- Poderá gravar qualquer ligação telefônica dos seus colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela DSK Capital para a atividade profissional de cada colaborador;

- Cancelará imediatamente o acesso concedido a Colaboradores desligados, afastados ou que tenham função alterada na gestora;

A utilização de softwares limita-se aos programas aprovados e devidamente homologados pelo Diretor de Compliance e Riscos da DSK Capital. A instalação de arquivos executáveis nas estações de trabalho ou na rede é terminantemente proibida, a não ser em casos em que haja expressa autorização do Diretor de Compliance e Riscos.

O Diretor de Compliance é responsável por manter, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos pela Instrução CVM 558/15, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções.

V. <u>Utilização do Correio Eletrônico (E-mail)</u>:

É proibida a utilização do correio eletrônico para:

(a) envio de mensagens ofensivas, difamatórias, preconceituosas, ou que possam causar hostilidade de qualquer espécie (de conteúdo religioso, sexual, político ou racial), ou que comprometam a imagem da DSK Capital;

(b) envio de mensagens por outros usuários que não os responsáveis pelo login e pela senha de acesso ao sistema;

(c) envio de mensagens que solicitem inscrição em listas de distribuições de mensagens na internet de assuntos não relacionados aos negócios da DSK Capital;

(d) envio de mensagens com o objetivo de prejudicar o serviço de indivíduos e/ou empresas (quantidade ou tamanho excessivo de mensagens, código malicioso etc.);

(e) envio de mensagens que levem o destinatário a incorrer em erro de identificação do emitente (se passar por outra pessoa);

(f) envio de mensagens cujo objetivo seja a venda de serviços e/ou produtos não relacionados aos negócios da DSK Capital;

(g) envio de mensagens, cujo conteúdo seja confidencial ou restrito à DSK Capital e não possa se tornar público;

(h) execução de arquivos anexados a mensagens recebidas de emitentes desconhecidos ou suspeitos;

(i) prática de ato que, de qualquer forma, possa ferir a legislação em vigor, as regras de sigilo bancário e direitos autorais;

(j) prática de ato em contraste com os deveres profissionais e com os interesses da DSK Capital, ou a fim de violar esta Política;

(k) recebimento de arquivos do tipo vídeo (*.avi, *.mpeg, entre outros).

(l) O recebimento de arquivos do tipo "executáveis" (programas) será controlado por programa antivírus contido nos equipamentos de controle de mensagens; e

(m) A assinatura de e-mail seguirá o seguinte padrão:

"Nome do Funcionário

DSK Capital

[telefone]

As informações contidas neste e-mail são confidenciais, podendo ser legalmente protegidas. Este e-mail foi elaborado exclusivamente para o destinatário. O acesso a este e-mail por terceiros não é autorizado. Se você não for o destinatário pretendido, qualquer divulgação, cópia, distribuição ou qualquer ação conduzida ou omitida com base neste e-mail é proibida e pode ser considerada ilegal. Caso tenha recebido essa mensagem por engano, por favor apague-a imediatamente e notifique o remetente por telefone. Obrigado.

The information in this e-mail is confidential and may be legally privileged. It is intended solely for the addressee. Access to this e-mail by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it is prohibited and may be unlawful. If you received this e-mail in error, please notify the sender immediately by telephone and destroy the original. Thank you."

VI. Segurança da informação e de dados:

Classificação das Informações: A fim de determinar o nível de proteção e garantir a segurança do compartilhamento de informações, a DSK Capital classifica as informações que transitam em seu ambiente físico e eletrônico da seguinte maneira: (a) pública - informação sobre a qual não há restrições quanto à divulgação, acessível a qualquer pessoa sem causar quaisquer consequências danosas aos processos da empresa; (b) interna - informação que a organização não tem interesse de divulgar, cujo acesso por parte de indivíduos externos deve ser evitado. Entretanto, caso esta informação seja disponibilizada, não haverá danos sérios à empresa; e (c) confidencial - informação interna da organização, cuja divulgação pode causar danos financeiros ou à imagem da empresa. A divulgação ainda pode gerar vantagens a eventuais concorrentes e perda de clientes.

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da DSK Capital, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da DSK Capital e circulem em ambientes externos à DSK Capital com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais. Qualquer informação sobre a DSK Capital, ou de qualquer natureza relativa às atividades da DSK Capital, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de Compliance e Riscos.

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

Procedimentos de Segurança: Como forma de prevenir, detectar e reduzir a vulnerabilidade a ataques digitais e vazamento de informações confidenciais, a DSK Capital segue, ainda, as seguintes medidas de

segurança:

- Não é permitida a conexão de equipamentos de informática ou software, não pertencentes à DSK Capital, na rede corporativa, sem a devida autorização do Diretor de Compliance e Riscos, que será precedida da anuência técnica do departamento de TI;
- O departamento de TI deve efetuar verificações semestrais na rede corporativa, para validar o acesso seguro aos recursos disponíveis e qualquer irregularidade encontrada deve ser imediatamente comunicada ao Diretor de Compliance e Riscos da DSK Capital;
- O bloqueio de acesso à rede será efetuado pelo departamento de TI sempre que solicitado pelo Diretor de Compliance e Riscos, ou caso seja detectado algum risco para a rede ou para os sistemas da DSK Capital.
- A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails e pastas de arquivos da DSK Capital devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros, Dessa forma, o Colaborador poderá ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.
- Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.
- Documentos considerados sensíveis são triturados previamente ao seu descarte, evitando assim o acesso fraudulento a nossas informações.
- A segregação das informações é realizada por meio de restrições ao acesso às informações de um departamento por Colaboradores de outro. Cada departamento possui um diretório próprio de armazenamento de documentos, o qual é acessado por meio de senhas e logins individuais.
- Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da DSK Capital

Acesso à base de dados: O acesso a sistemas, bases de dados e redes é restrito e definido em função do perfil de cada Colaborador da DSK Capital. O detalhamento do perfil de acesso de cada Colaborador (incluindo operadores e eventuais prestadores de serviços) é realizado no momento da contratação e criteriosamente analisado pelo Diretor de Compliance e Riscos para cada caso. A liberação do acesso a qualquer sistema, base de dados ou endereço de rede depende de prévia aprovação do Diretor de Compliance e Riscos. O acesso à base de dados está submetido às seguintes diretrizes:

(a) Tentativas para obtenção de acesso não autorizado (fraude de autenticação de usuário ou segurança de qualquer servidor, rede ou conta) não são permitidas. Inclui-se neste ponto o acesso a dados não disponíveis para o usuário, bem como a tentativa de conexão a servidores ou contas cujo acesso não tenha sido expressamente autorizado e situações que coloquem à prova a segurança de outras redes;

(b) Tentativas de interferência nos serviços de qualquer outro usuário, servidor ou rede não são permitidas. Inclui-se neste ponto ataques do tipo “negativa de acesso”, congestionamento em redes, bem como tentativas deliberadas de sobrecarga e/ou invasão de um servidor;

(c) Materiais de conteúdo inapropriado (ex.: pornografia) não podem ser expostos, armazenados, distribuídos, editados ou gravados por meio do uso dos recursos computacionais da rede;

(d) A pasta transferência (ou similar) não deverá ser utilizada para armazenamento de arquivos que contenham materiais de natureza sigilosa ou sensível;

(e) A armazenagem de arquivos inerentes às atividades profissionais desempenhadas por cada um dos Colaboradores da DSK Capital nos servidores de arquivos é obrigatória. Tal medida visa assegurar a realização de backups de segurança; e

(f) A varredura simples ou em massa, visando a descoberta de endereços ou portas e/ou qualquer ataque ou tentativa de invasão é terminantemente proibida.

Backup e Restore de Arquivos:

- Sistema de Armazenamento de Dados. A DSK Capital adota o sistema de servidores remotos da *Microsoft Office 365 Business* para gerenciar suas informações. Nesse sistema, os arquivos eletrônicos ficam armazenados remotamente em servidores seguros e com redundância. Por meio desse sistema, somente usuários com senha conseguem acessar as informações e documentos, evitando que pessoas não autorizadas tenham acesso a tais informações. O acesso é feito com uso de senhas pessoais e intransferíveis, com procedimento de verificação em 2 (duas) etapas (login e senha) e por meio de equipamento (computador, celular, tablet) previamente cadastrado e aprovado. Qualquer atividade na rede é monitorada, identificada (usuário, computador e IP que acessou o sistema), e pode ser revertida ou bloqueada. O sistema possui, ainda, diferentes níveis de acesso aos arquivos, sendo possível realizar restrições de nível de pasta e arquivo o que garante maior confidencialidade das informações e redução do risco de uso indevido dessas. Por fim, o sistema realiza um backup diário das informações armazenadas localmente e possui redundância no armazenamento das informações e arquivos nos servidores remotos, de modo que na ocorrência de problemas como perda de dados, os arquivos e as informações podem ser recuperados rapidamente dos servidores remotos sem grandes interrupções nas atividades dos Colaboradores.
- Os Colaboradores estão obrigados a armazenar toda e qualquer informação relativa às suas atividades no sistema de servidor remoto, tendo em vista que não há garantia de *backup* para arquivos armazenados nas estações de trabalho (desktops ou notebooks) fora de tais sistemas. O armazenamento de informações e documentos em desacordo com esta Política será considerado violação e sujeitará o Colaborador às penalidades cabíveis;
- O restore de dados deve ser solicitado ao departamento de TI e será realizado de acordo com os procedimentos específicos do servidor remoto; e
- As mídias (suprimentos) serão adquiridas pela DSK Capital, sempre que necessário.

VII. Responsabilidade e Procedimentos Internos para Tratamento de eventual incidente de dados

Responsabilidade pelo tratamento de incidentes de dados: O Diretor de Compliance e Risco será o responsável para tratar e responder questões relacionadas à segurança cibernética. Qualquer processo ou ativo classificado como confidencial será considerado como vulnerável para fins de segurança cibernética, sendo classificado internamente com alto grau de ameaça institucional em caso de eventual ataque cibernético.

Para fins de monitoramento, o Diretor de Compliance e Risco da DSK Capital realiza, periodicamente, testes de segurança e procedimentos para detectar falhas e vulnerabilidades. Adicionalmente, a DSK Capital (i) mantém inventários atualizados de hardware e software por ela detidos; (ii) mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizados; (iii) monitora diariamente as rotinas de backup, executando testes regulares de restauração dos dados; e (iv) analisa regularmente as trilhas de auditoria criadas, de forma a permitir a rápida identificação de ataques, sejam internos, sejam externos.

No caso concreto de um ataque cibernético amplo nas redes da DSK Capital, o Diretor de Compliance e Riscos deverá contatar imediatamente os Colaboradores da DSK Capital, bem como assessoria especializada para resolver a questão no menor tempo possível. Neste cenário, os Colaboradores deverão utilizar instalações de contingência até a normalização dos serviços, as quais obedecerão às regras de controle de acesso previstas nesta Política. Em se tratando de um ataque individual a um determinado Colaborador, a DSK Capital deverá disponibilizar novos equipamentos para a continuidade da prestação dos serviços por parte daquele Colaborador.

Eventual incidente cibernético deverá ser documentado por escrito em relatório elaborado pelo Diretor de Compliance e Riscos, no qual constarão as descrições do incidente e as medidas tomadas para resolver tal incidente, e deverá ser arquivado na sede da DSK Capital para fins de evidência em caso de eventuais questionamentos. Em caso de divulgação indevida de qualquer informação confidencial, o Diretor de Compliance e Riscos irá apurar o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

Procedimento: Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela DSK Capital para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme descritos nesta Política, na eventualidade de ocorrer o vazamento de quaisquer informações, ainda que de forma involuntária, o Diretor de Compliance e Riscos deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de Compliance e Riscos, primeiramente, identificará se a Informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de Compliance e Riscos procederá da seguinte forma:

1. No caso de vazamento de Informações relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

2. No caso de vazamento de Informações relativas aos cotistas:

Neste caso, o Diretor de Compliance e Riscos procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, o Diretor de Compliance e Riscos ficará à inteira disposição para auxiliar na solução da questão.

VIII. Disposições Gerais

Os procedimentos previstos nesta Política, conforme mencionados anteriormente, serão revisados anualmente pela DSK Capital, ou quando houver alteração na regulação referente à segurança cibernética. Em tais revisões, serão atualizadas as avaliações de riscos, vulnerabilidades e ameaças identificadas originalmente.

O descumprimento de quaisquer das regras estabelecidas nesta Política deverá ser levado, imediatamente, para a apreciação do Diretor de Compliance e Riscos, podendo, conforme aplicável, resultar em demissão por justa causa do Colaborador, sem prejuízo da reparação dos danos a que der causa, inclusive os de ordem moral, bem como das responsabilidades civil e criminal respectivas, apurados em regular processo judicial ou administrativo. Eventuais alterações desta Política serão prontamente comunicadas a todos os

Colaboradores da DSK Capital e disponibilizadas no website da DSK Capital.

Eventuais dúvidas ou questionamentos devem ser diretamente encaminhados ao Diretor de Compliance e Riscos conforme abaixo:

Diego Stark

E-mail: diegostark@dskcapital.com.br.