THE CARLYLE GROUP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

TCG GESTOR LTDA

Abril de 2020 – Versão 1.0

ÍNDICE

RESUMO 3
OBJETIVO 3
PREMISSAS E DEFINIÇÕES 4
PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO 4
PROGRAMA DE SEGURANÇA DO TCG GESTOR 7
MONITORAMENTO E TESTES DE CONTINGÊNCIA 16
PLANO DE RESPOSTA 16
TREINAMENTO 17
VIGÊNCIA E ATUALIZAÇÃO 17

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

RESUMO

A Política de Segurança da Informação e Segurança Cibernética ("Política") do TCG Gestor Ltda. ("TCG Gestor"), aplica-se a todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança com o TCG Gestor (em conjunto os "Colaboradores" e individualmente o "Colaborador") , prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento do TCG Gestor, ou que acesse informações a ele pertencentes. Todo e qualquer usuário de recursos computadorizados tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática do TCG Gestor.

TCG Gestor é integrante do The Carlyle Group ("Carlyle"), um grupo global de gestão de ativos e valores mobiliários, que atua como gestor de fundos de investimento especializados e outros veículos de investimento, que investem em uma vasta gama de setores, localidades geográficas, classes de ativos e estratégias de investimento.

O TCG Gestor é um administrador de carteira de valores mobiliários, devidamente registrado perante a Comissão de Valores Mobiliários ("CVM") na categoria de "gestor de recursos", nos termos da Instrução da CVM n° 558, de 26 de março de 2015 ("Instrução CVM 558"), focado na gestão de fundos de investimentos em participações (*private equity*), cuja carteira é composta por: (a) principalmente, ativos altamente ilíquidos, tais como ações e outros valores mobiliários emitidos por companhias não listadas e ações emitidas por companhias listadas, desde que adquiridas como parte de estratégia de *private equity*; e (b) em menor escala, por ativos líquidos adquiridos pelos fundos geridos, utilizados para gestão do caixa dos fundos.

Em linha com as principais discussões e preocupações do mercado, a Política tem como base princípios e procedimentos que asseguram a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pelo TCG Gestor.

Sem prejuízo do disposto na presente Política, o TCG Gestor, como entidade parte do Carlyle, está sujeito ao disposto na Acceptable Use Policy do Carlyle que estabelece diretrizes e regras de utilização dos recursos das entidades afiliadas ao Carlyle ("Política de Uso"), na *Privacy Policies and Procedures* que estabelece as regras de confidencialidade, privacidade e segurança da informação a todos os colaboradores do Carlyle ("Política de Privacidade") e *Privacy Notice and Safeguarding Policies and Procedures* ("Políticas e Procedimentos de Notificação" e, em conjunto com esta Política, a Política de Uso e a Política de Privacidade, "Políticas Globais").

OBJETIVO

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética do TCG Gestor, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para as atividades do TCG Gestor.

Em atenção aos dispositivos da Instrução CVM 558 e do Código ABVCAP/ANBIMA de Regulação e Melhores Práticas para o Mercado de FIP e FIEE, o TCG Gestor procurou identificar os eventos

com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade, com o propósito de mitigar os riscos à sua atividade.

PREMISSAS E DEFINIÇÕES

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidencias (conforme abaixo definido), o que é de extremo valor para o TCG Gestor, dado o princípio fundamental de confiança que trabalha para manter junto aos seus clientes, o TCG Gestor utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança da ANBIMA, datado de dezembro de 2017.

Adiante, o TCG Gestor abordará os principais mecanismos e procedimentos de prevenção às ameaças ao seu patrimônio, à sua imagem e, principalmente, aos seus negócios.

Todas as diretrizes aqui dispostas são de responsabilidade do Diretor de Compliance, Prevenção à Lavagem de Dinheiro e Gestão de Riscos ("Diretor de Compliance") do TCG Gestor.

Ademais, para implementação e monitoramento contínuo da presente Política, o TCG Gestor conta com o suporte e a estrutura da equipe de TI global do Carlyle.

Para fins da presente Política, são consideradas "Informações Confidenciais":

(i) Informações proprietárias ou materiais, não-públicas, do TCG Gestor, de seus Colaboradores, dos ativos geridos e/ou de seus clientes; e

(ii) Qualquer outra informação que tenha sido fornecida ou obtida com obrigação de confidencialidade e/ou de fontes não-públicas, no contexto da atuação do TCG Gestor e de seus Colaboradores.

PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Conforme previsto no Código de Ética e Conduta do TCG Gestor ("Código de Ética"), o TGC Gestor adota diretrizes de confidencialidade com relação às Informações Confidenciais utilizadas em suas atividades, inclusive aquelas fornecidas pelos seus clientes.

Tais Informações Confidenciais TCG Gestor não serão utilizadas para nenhuma finalidade além daquelas imprescindíveis para a prestação dos serviços de gestão de carteiras pelo TCG Gestor, exceto em caso de exigência legal ou determinação judicial – hipóteses nas quais o cliente titular da informação será previamente notificado.

Todos os Colaboradores estão sujeitos a observarem as regras de confidencialidade, sendo vedada a divulgação de quaisquer Informações Confidenciais às quais tenham acesso a quaisquer terceiros (com exceção das hipóteses previstas abaixo), sob pena de aplicação das sanções previstas no Código de Ética.

Para garantir a proteção das informações, o TCG Gestor conta com estrutura física e eletrônica, bem como procedimentos de segurança referentes às normas de armazenamento de documentos e informações e controle de acesso.

1. Divulgação de Informações

As Informações poderão ser compartilhadas pelo TCG Gestor com outras entidades pertencentes ao Carlyle, desde que tal compartilhamento se limite às Informações Confidenciais referentes a transações realizadas pelo TCG Gestor.

As Informações Confidenciais poderão ser compartilhadas com terceiros nas seguintes hipóteses:

(i) Quando necessário par os prestadores dos serviços relacionados à administração e processamento de transações, incluindo advogados, contadores, consultores e auditores;

(ii) Quando houver consentimento do Diretor de Compliance ou do cliente, conforme aplicável;

(iii) A qualquer pessoa devidamente constituída como representante do cliente;

(iv) Em cumprimento de ordem de autoridade Federal, Estadual ou Municipal e/ou legislação aplicável, mediante expressa autorização do Diretor de Compliance;

(v) Em colaboração com investigações criminais, civis ou regulatórias, ou em caso de intimação para prestar as informações emitida por autoridade Federal, Estadual ou Municipal, mediante expressa autorização do Diretor de Compliance; e

(vi) No âmbito de defesa apresentada em processo judicial ou administrativo perante as autoridades reguladoras, mediante expressa autorização do Diretor de Compliance.

Em qualquer dos casos, a Informação somente poderá ser utilizada para cumprir o propósito pelo qual se deu a sua divulgação. No caso de compartilhamento de informações fornecidas por clientes, quando assim exigido nos termos da legislação e regulamentação aplicável, o cliente titular daquela informação será devidamente notificado sobre tal compartilhamento.

É expressamente vedado a qualquer Colaborador:

(i) Fazer upload ou distribuir Informações Confidenciais de qualquer rede do TCG Gestor ou do Carlyle para redes e/ou armazenamentos externos, tais como servidores, redes *cloud*, sites ou qualquer outro diretório, sem autorização prévia;

(ii) Distribuir Informações Confidenciais para qualquer terceiro que não seja uma pessoa autorizada a ter acesso a tais informações;

(iii) Salvar, imprimir, baixar, distribuir ou arquivar qualquer documento ou pasta que contenha Informações Confidenciais, excetuadas situações específicas que referida ação seja necessária no curso normal dos negócios e desde que devidamente autorizada e arquivada.

Adicionalmente, com objetivo de resguardar tais Informações Confidenciais e evitar transmissões não intencionais, é recomendado aos Colaboradores que observem as seguintes diretrizes:

(i) Evitar discussões envolvendo informações sensíveis ou Informações Confidenciais com pessoas que não necessitem ter acesso a tais informações;

(ii) Evitar discussões envolvendo informações sensíveis ou Informações Confidenciais em ambientes públicos (tais como lobbys, elevadores, taxis e outros meios de transporte compartilhado, aviões, aeroportos, restaurantes, etc.);

(iii) Evitar uso de alto-falantes em conversas e conferências telefônicas que envolvam discussão de informações sensíveis ou Informações Confidenciais, especialmente quando próximo de pessoas que não devam ter acesso a tais informações;

(iv) Uso de codinomes para se referir a projetos sensíveis;

(v) Antes de imprimir qualquer documento contendo Informações Confidenciais, certificar-se que a impressora somente é acessível a pessoas que possam tomar conhecimento daquela informação;

(vi) Certificar-se que documentos e outros materiais contendo Informações Confidenciais sejam descartados de maneira apropriada;

(vii) Não deixar qualquer material que contenha Informações Confidenciais em locais de livre acesso ou sem devida supervisão, incluindo salas de reunião, em cima da estação de trabalho, refeitórios ou outros locais comuns dos escritórios do TCG Gestor ou do Carlyle.

Caberá ao Diretor de Compliance acompanhar e supervisionar a implementação e o cumprimento das diretrizes de privacidade, bem como a justificativa para o compartilhamento.

2. Controle de Informações Confidenciais

O acesso a Informações Confidenciais mantidas na rede do TCG Gestor e do Carlyle será controlado através do login individual atribuído a cada Colaborador e uso de senha. Os requisitos a serem observados para registro de Informações Confidenciais incluem, dentre outros:

(i) Uso de servidores do próprio Carlyle ou prestadores de serviços pré-aprovados;

(ii) Procedimentos de segurança dos servidores com base nos critérios descritos nessa Política, mantidos sempre atualizados;

(iii) Monitoramento constante de acesso remoto à tais Informações Confidenciais de maneira a identificar acessos suspeitos e potenciais fragilidades;

(iv) Manutenção de Informações Confidenciais em redes separadas das demais informações armazenadas nos servidores;

(v) Restrição no uso de pastas compartilhadas, com acesso controlado e sempre pré-aprovado;

(vi) Quando necessário, uso de criptografia de acordo com padrões mais recentes para garantir segurança da Informação Confidencial.

O Diretor de Compliance, em conjunto com o time de compliance do Carlyle, será responsável por monitorar, registrar e controlar a transmissão de Informações Confidenciais entre Colaboradores e com terceiros.

Informações Confidenciais mantidas em meio físico, tais como diretórios, arquivos e outros formatos de registro, também terão seu acesso controlado e restrito a determinados Colaboradores que necessitem ter acesso à tais informações.

O Diretor de Compliance também será responsável por atribuir as permissões de acesso às Informações, mantendo uma lista de pessoas com autorização de acesso.

3. Testes e Procedimentos de Segurança

Os procedimentos para verificação da segurança das Informações Confidenciais armazenadas em formato eletrônico pelo TCG Gestor estão descritos nos itens a seguir.

PROGRAMA DE SEGURANÇA DO TCG GESTOR

1. Identificação de Riscos:

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

(i) *Malware* – *softwares* desenvolvidos para corromper computadores e redes:

(a) Vírus: *software* que causa danos à máquina, rede, *softwares* e banco de dados;

(b) Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;

(c) *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e

(d) *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

(ii) Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

(a) *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

(b) *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

(c) *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

(d) *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

(e) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

(iii) Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

(iv) Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, o TCG Gestor pode estar sujeito a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar o perdimento e/ou adulteração de dados e Informações.

2. Ações de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade paro TCG Gestor, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional, em caso de incidente de segurança.

Deste modo, o TCG Gestor segrega as informações, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classifica-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

(i) *Green Flag*:

(a) Quaisquer informações e/ou dados que o TCG Gestor teve acesso ou conhecimento por ser de domínio público ("Informação Pública");

(b) Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou

(c) Quaisquer informações e/ou dados que tenham sido obrigatoriamente divulgadas por força de lei ou ordem de autoridade competente.

(ii) *Yellow Flag*:

(a) Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, em data anterior à determinada para a divulgação (Ex. Data de Divulgação);

(iii) *Red Flag*:

Todas as Informações Confidenciais, a saber:

(a) know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pelo TCG Gestor;

(b) operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pelo TCG Gestor; e

(c) 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 do TCG Gestor e/ou de seus sócios e clientes.

A partir da definição acima, o TCG Gestor se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: *Red Flag*, *Yellow Flag* e *Green Flag*.

Além da classificação de acordo com a sensibilidade das informações armazenadas, o TCG Gestor monitora a ocorrência de determinados eventos que representam um grave risco de segurança, tais como elencadas abaixo ("*Red Flags* Situacionais"):

(i) Recebimento de notificação – verificável – de um cliente afirmando que tenha sido vítima de roubo de identidade;

(ii) Recebimento de notificação – verificável – enviada por uma autoridade governamental, depositário ou outro prestador de serviço vinculado sobre roubo de identidade relacionada a uma determinada conta individual;

(iii) Devolução de correspondência física ou eletrônica enviada pelo TCG Gestor a determinado cliente ou recebimento de uma notificação de um cliente individual sobre o não recebimento de uma correspondência esperada;

(iv) Pedidos ou comportamentos de movimentação individual de contas em desacordo com o padrão habitual;

(v) Tentativa de alteração dos dados da conta por um contato não autorizado;

(vi) Documentos de identificação de um cliente ou outros documentos que estejam incompletos ou com sinais de adulteração ou falsificação;

(vii) A prestação de informações incoerentes por um cliente em formulários ou durante as conversas com os Colaboradores; e

(viii) Relutância dos clientes em participar de processos contábeis regulares utilizados para estabelecer e manter os relacionamentos com os clientes e prestadores de serviços.

3. Verificação e Tratamento das *Red Flags* Situacionais

A verificação da ocorrência das *Red Flags* Situacionais é realizada internamente pelo TCG Gestor, seguindo, inclusive, as diretrizes globais do Carlyle. Para verificar com segurança a identidade dos clientes, o TCG Gestor executa as rotinas descritas no "*Custumer Identification Program*" implementado pelo Carlyle a nível global.

Todos os processos de abertura e encerramento de contas são supervisionados pelo Diretor de Compliance, que, entre outras atribuições é responsável pela verificação das informações de contato e sobre a completude e a exatidão de formulários e outros documentos pertinentes, bem como informações e dados para a realização de transferências bancárias

É de responsabilidade de todos os Colaboradores informar imediatamente a seus superiores ou ao Diretor de Compliance quaisquer suspeitas acerca da verificação de *Red Flags* Situacionais ou qualquer outra atividade suspeita que possa ser indicativa de roubo de identidade para a qual não haja justificativa.

Sempre que for identificada a ocorrência de uma *Red Flag* Situcional ou outras situações supeitas, a equipe liderada pelo Diretor de Compliance investigará as especificidades de cada caso para determinar a melhor estratégia de mitigação de danos, a qual poderá incluir um ou mais dos seguintes procedimentos:

(i) Monitorar cuidadosamente a(s) conta(s) afetada(s) em busca de evidências da ocorrência roubo de identidade ou outras atividade imprópria;

(ii) Notificar os clientes afetados;

(iii) Alteração de senhas, códigos de segurança e/ou outros controles adotados para prevenir atividades não autorizadas;

(iv) Recusa de abertura de uma nova conta e/ou encerramento de uma conta existente;

(v) Notificação às competentes autoridades governamentais;

(vi) Alterar as diretrizes previstas nesta Política; e/ou

(vii) Qualquer outra providência que se mostre adequada ao caso concerto, até mesmo a opção de que nenhuma providência deva ser tomada.

Todas as notificações verificadas ou suspeitas de ocorrência de *Red Flags* Situacionais serão registradas pela equipe gerida pelo Diretor de Compliance, que será responsável pelo

arquivamento e guarda da documentação relativa a tais registros.

4. Propriedade dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade do TCG Gestor. Não é permitida a utilização de *notebooks*, *tablets* ou outros *hardwares* para operações no âmbito das Gestoras, salvo expressa permissão do Diretor de Compliance.

5. Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores do TCG Gestor têm por objetivo o desempenho das atividades profissionais, não devendo ser utilizado para quaisquer outros fins.

Todo o processo de criação e exclusão de usuário, instalação de *softwares* e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela equipe de TI, mediante aprovação do Diretor de Compliance.

A disponibilização e uso dos computadores do TCG Gestor respeitam as seguintes regras:

(i) A cada novo Colaborador, o Diretor de Compliance autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;

(ii) Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela equipe de TI;

(iii) Cada computador será vinculado a um usuário, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da equipe de TI, mediante supervisão e aprovação do Diretor de Compliance*;*

(iv) A identificação do usuário é feita através do *login* e senha. Cada login e senha somente podem ser utilizados pelo usuário ao qual foram associados, que será responsável pelas ações decorrentes de sua utilização e encarregado de preservar a sua segurança;

(v) O mesmo login e a mesma senha utilizados para acessar os equipamentos disponibilizados serão necessários para acessar as funcionalidades dos sistemas do TCG Gestor, inclusive através de acesso remoto; e

(vi) A senha possui validade e sua troca será solicitada automaticamente quando da expiração da mesma.

Para realizar o acesso remoto à rede do TCG Gestor será exigida do Colaborador uma autenticação de dois fatores, sendo um deles a utilização do respectivo login e senha e o outro uma autenticação via certificado – a ser disponibilizado pela equipe de TI do TCG Gestor a cada Colaborador, individualmente.

6. Softwares

A implantação e configuração de *softwares* pelo TCG Gestor e o Carlyle em geral respeitam as seguintes regras:

(i) Todos os *softwares*, programas básicos (sistema operacional e ferramentas) e componentes físicos são licenciados e serão implantados e configurados pela equipe TI, mediante supervisão e aprovação do Diretor de Compliance.

(ii) É desabilitado aos usuários instalar novos programas ou alterar configurações sem a assistência da equipe de TI, que, conforme o caso, poderá solicitar aprovação do Diretor de Compliance.

(iii) É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores.

(iv) Somente é permitido o uso de equipamentos homologados e devidamente contratados pelo TCG Gestor.

(v) A utilização de equipamentos pessoais por terceiros nas instalações do TCG Gestor e a conexão destes na rede interna à Internet requer autorização prévia e expressa do Diretor de Compliance. Os Colaboradores deverão receber autorização da equipe de TI antes de conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet.

(vi) A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa do Diretor de Compliance.

7. Registros

O TCG Gestor mantém por 05 (cinco) anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam *softwares*, *hardwares* ou acessos que não sejam autorizados.

Nesse sentido, através dos logs, o TCG Gestor consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme 4º, §8º, da Instrução CVM n.º 558/15.

8. Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento, bem como do login e senha que lhe tenham sido atribuídos.

O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pelo TCG Gestor.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

(i) Não compartilhar nem divulgar sua senha a terceiros;

(ii) Não transportar Informações Confidenciais do TCG Gestor em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;

(iii) Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);

(iv) Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;

(v) Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e

(vi) Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pelo TCG Gestor.

9. Outras Proteções aos Computadores

(i) Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente).

(ii) "*Log-off*" automático por inatividade durante o período de 24 horas.

(iii) Bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores.

(iv) Bloqueio do acesso a sites de armazenamento de dados em Nuvem (*Cloud Service*) não aprovados pelo Comitê de Ética, Risco e Compliance.

(v) Bloqueio de sistemas de gerenciamento de computador à distância.

10. Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia do TCG Gestor, este deve sempre resguardar a imagem do TCG Gestor, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais, exceto quando necessário, ou, de fontes não conhecidas.

O usuário é proibido de acessar endereços de internet (sites) que:

(i) Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes.

(ii) Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.

(iii) Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.

(iv) Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

(v) Outros sites que, no entendimento do TCG Gestor, sejam considerados inapropriados.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

Caberá ao TCG Gestor a prerrogativa de bloquear o acesso a quaisquer sites considerados inapropriados.

É proibido o uso de serviços de mensagem instantânea, além do Skype Business, para a condução dos negócios do TCG Gestor. Outros serviços de mensagens instantâneas acessados a partir dos dispositivos disponibilizados pelo TCG Gestor estarão sujeitos a registro e controle por parte da equipe de TI, independentemente da finalidade do seu uso.

11. Bloqueio de endereços de Internet

Periodicamente, a equipe de TI, sob a orientação do Diretor de Compliance, irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com as Políticas e com o Código de Ética.

12. Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

O TCG Gestor disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais.

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence ao TCG Gestor.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com o TCG Gestor.

Se houver necessidade de troca de endereço, a alteração será realizada pela equipe de TI, mediante autorização e supervisão do Diretor de Compliance.

13. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pelo TCG Gestor mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico do TCG Gestor.

14. Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional no TCG Gestor.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

(i) Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;

(ii) Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;

(iii) Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para o TCG Gestor, a sugestão deve ser encaminhada para o Diretor de Compliance, que definirá a sua publicação ou não;

(iv) Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;

(v) Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;

(vi) Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;

(vii) Defendam ou possibilitem a realização de atividades ilegais;

(viii) Sejam ou sugiram a formação ou divulgação de correntes de mensagens;

(ix) Possam prejudicar a imagem do TCG Gestor; e

(x) Sejam incoerentes com o Código de Ética.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico do TCG Gestor é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome do TCG Gestor.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

O Colaborador deve ser diligente em relação:

(i) Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);

(ii) Ao nível de sigilo da informação contida na mensagem;

(iii) Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos; e

(iv) Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas úteis sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

15. Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria, a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da equipe de TI, mediante supervisão do Diretor de Compliance.

MONITORAMENTO E TESTES DE CONTINGÊNCIA

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela equipe de TI, sob supervisão do Diretor de Compliance. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que o TCG Gestor esteja preparado para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios do TCG Gestor.

PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, o TCG Gestor desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política.

Estas providências consistem em:

1. Equipe de TI (Sob Supervisão Diretor de Compliance):

(i) Verificação e Auditoria dos Logs;

(ii) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;

(iii) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;

(iv) Desinstalação de *software*;

(v) Execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;

(vi) Formatação e reconstrução do sistema operacional;

(vii) Substituição física de dispositivos de armazenamento;

(viii) Reconstrução de sistemas e redes;

(ix) Restauração de dados provenientes do *backup* realizado diariamente; e

(x) Outras ações que se mostrem necessárias após avaliação do caso concreto.

2. BackOffice:

(i) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos do TCG Gestor e dos fundos geridos; e

(ii) Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos do TCG Gestor e dos fundos geridos resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados, documentados e formalizado no Relatório de Controles Internos do TCG Gestor.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética do TCG Gestor.

TREINAMENTO

Todos os Colaboradores deverão passar por um treinamento sobre as práticas e procedimentos previstos nas Políticas Globais trimestralmente, para assegurar a efetividade dos procedimentos de segurança adotados pelo TCG Gestor e pelo Carlyle.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada periodicamente, pelo menos 01 (uma) vez ao ano, 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.

O objetivo principal do processo de revisão dessa Política é manter sempre atualiza a metodologia de avaliação de risco, as implementações de proteção e prevenção, os monitoramentos e testes e os planos de resposta.

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/ME sob o nº _____, declaro que li e estou plenamente de acordo com as disposições da Política de Segurança da Informação e Segurança Cibernética aprovados TCG Gestor Ltda. em abril de 2020. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

São Paulo, _____ de _____ de 20__.

_____

[Colaborador]