GRUPO GIANT STEPS

Política de Segurança Cibernética e da Informação

DIRETORIA DE RISCO & COMPLIANCE

SET-20

gscap.com.br

GRUPO GIANT STEPS

GIANT STEPS CAPITAL INVESTIMENTOS LTDA.
CNPJ/MF nº 17.021.922/0001-88

Rua Elvira Ferraz, 250 – cj 407
ED. FL OFFICE
CEP: 04552-040 – São Paulo/SP
Tel: + 55 (11) 2533 2820

gscap.com.br

ZEITGEIST TECH INVESTIMENTOS LTDA.
CNPJ/MF nº 04.870.394/0001-90

Rua Elvira Ferraz, 250 – cj 407
ED. FL OFFICE
CEP: 04552-040 – São Paulo/SP
Tel: + 55 (11) 2533 2820

gscap.com.br

Canal de denúncia

denuncia@gscap.com.br

Índice

V20.1.0

V20.1.1

1. Introdução

Com o objetivo de preservar a segurança cibernética e as informações em posse do Grupo Giant Steps, a mesma adotou e adicionou na sua instituição a Diretoria de Segurança Cibernética e da Informações com colaborador qualificado a fim de tratar o assunto com o maior relevo possível. O Grupo Giant Steps adota todas as medidas cabíveis, dentro da sua capacidade, objetivando maior rigidez para mitigar os riscos de invasões que resultem em vazamento de informações sigilosas.

Ainda, o Grupo Giant Steps investe em seus colaboradores, adquirindo *softwares* específicos para o controle eficiente, se necessário, e realiza treinamento periódico para os atualizar sobre a preservação dos dados sigilosos.

A presente política é baseada em princípios e diretrizes, resguardando detalhes de informações sigilosas de segurança e controle, para segurança interna. O presente conjunto de regras e procedimentos é endereçada à todos os colaboradores e parceiros do Grupo Giant Steps Capital que devem cumpri-la integralmente.

Respectiva política está em acordo com a lei 13.709/18, resolução n. 4.658/18 do Banco Central do Brasil, Código Civil Brasileiro lei 10.406/02 e as diretrizes estabelecidas pela Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais (ANBIMA).

2. Negócio e Responsabilidade

Tendo em vista a atividade financeira do Grupo Giant Steps que atua como Gestor e Distribuidor dos próprios fundos de investimentos a mesma mantém todos os dados de clientes, parceiros e colaboradores classificados de acordo com o sigilo e relevância que envolve respectiva informação.

Ademais, todos os dados de clientes, parceiros e colaboradores são coletados visando obedecer às obrigações legais impostas pelos órgãos reguladores e controladores para a execução das atividades do grupo. Os dados coletados pelos clientes, parceiros e

colaboradores devem ser fornecidos com a ciência dos mesmos e visam, principalmente, efetuar e atualizar dados cadastrais e fornecer os requisitos para o devido processo de verificação da área de Compliance.

O descarte das informações será realizado logo após o cumprimento das exigências procedimentais e legais, quando permitido por lei, evitando-se o armazenamento de informações indevidas ou sem necessidade.

O Grupo Giant Steps é responsável em coletar e armazenar os dados fornecidos pelos clientes e parceiros. Os dados coletados para efeito de cadastro e, eventualmente, para processos de *Know Your Client* (KYC), são transmitidos ao administrador o Banco BNY Mellon Serviços Financeiros Distribuidora de Títulos e Valores Mobiliários S.A. com sede na Cidade e Estado do Rio de Janeiro Av. Presidente Wilson n. 231 e inscrito no CNPJ sob o n. 02.201.501/0001-61 que também possui o dever e obrigação de tratar as informações prestadas de acordo com o sigilo e relevância.

3. Boas Práticas

O grupo Giant Steps adota procedimentos estabelecidos em âmbito nacional e internacional para assegurar as informações que lhe foi confiada seguindo boas práticas tais, como, e não exclusivamente:

O grupo Giant Steps Capital mantém controle das informações de dados que lhe são fornecidos por clientes, parceiros e colaboradores. Os colaboradores que possuem acesso às informações serão somente aquelas que necessitem da mesma para sua atividade. Sendo assim o grupo adota a política estabelecida como "*Need to Know*". Caberá ao Diretor de Segurança Cibernética e da Informação e ao Diretor de Compliance fornecer ou não as informações mínimas aos colaboradores quando necessário.

Os Colaboradores deverão zelar pela conservação do computador utilizado, devendo, para tanto, realizar periodicamente a verificação da existência de vírus, bem como a manutenção do antivírus atualizado. Sendo constatada a presença de vírus ou quaisquer outras

anomalias, o Colaborador deverá comunicar imediatamente a Diretoria de Risco e Compliance do Grupo Giant Steps.

As senhas de caráter sigiloso, pessoal e intransferível serão fornecidas pelo Direto de Segurança Cibernético e da Informação aos Colaboradores do Grupo Giant Steps para acesso aos computadores, à rede corporativa e ao E-Mail Corporativo. Em nenhuma hipótese, as senhas deverão ser transmitidas a terceiros, sendo os respectivos Colaboradores responsáveis pela manutenção de cada senha de sua titularidade com as suas respectivas características.

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

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora. É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pelo Diretor de Segurança Cibernética e da Informação.

Não é permitida a instalação de nenhum software ilegal ou que possua direitos autorais protegidos. A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente ao Diretor de Segurança Cibernética e da Informação. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos profissionais e pessoais.

4. Atribuições do Diretor

Conforme estabelecido pelas leis vigentes o grupo Giant Steps Capital conta com Diretor de Segurança Cibernética e da Informação cujas atribuições principais são:

(i) preservar a segurança dos dados e informações sigilosas, utilizando todos os meios possíveis;

(ii) estabelecer processos e controles de segurança;

(iii) auxiliar a Diretoria de Risco e Compliance no mapear dos riscos de vulnerabilidades;

(iv) descrever e apresentar aos demais colaboradores os cenários de ameaça;

(v) monitorar os processos previamente definidos;

(vi) criar planos de contingência em caso de vazamento de dados e invasões;

(vii) zelar pela segurança dos computadores internos.

5. Monitoramento

O Diretor de Segurança Cibernética e da Informação deve encaminhar às Diretorias integrantes do Grupo Giant Steps, até o último dia útil do mês de março de cada ano, relatório (cf. anexo I) relativo ao ano civil imediatamente anterior à data de entrega, contendo:

(i) as conclusões dos exames efetuados;

(ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e

(iii) a manifestação do Diretor de Segurança Cibernética e da Informação a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las. Respectivo registro

visa analisar os principais riscos e vulnerabilidades da empresa, criando os respectivos planos de ação quando necessários.

Referido relatório ficará disponível para a Comissão de Valores Mobiliários - CVM na sede do Grupo Giant Steps e no website www.gscap.com.br.

6. Controle de Incidentes

De acordo com as políticas internas estabelecidas será considerado como incidente o erro ou falha humana ou de sistema em qualquer procedimento operacional do Grupo Giant Steps que poderia ter sido evitado com a adoção de práticas ou comportamentos compatíveis com o negócio.

Os incidentes são classificados de acordo com o impacto ou perspectiva de impacto negativo para seus membros, clientes, fornecedores e parceiros.

Os eventuais incidentes serão descritos caracterizados em relatório próprio que descreverá o objeto do controle ou do incidente, seus resultados e plano de ação se houver necessidade. Este documento ainda contará com a data, a área operacional envolvida, o prazo para a resolução de eventuais problemas e o risco auferido para a gestora, clientes e fornecedores.

O documento poderá conter as recomendações e orientações fornecidas pela área de Compliance e plano de ação.

Sempre que for avaliado incidentes ou potenciais incidentes que envolvam clientes, parceiros e colaboradores os mesmos serão informados com a maior brevidade possível, cabendo ao Grupo Giant Steps Capital empreender seus maiores esforços para mitigar os danos.

O Grupo Giant Steps conta com Plano de Contingência e Continuidade de Negócio que visa acionar rapidamente ações diretas e estudadas contra incidentes e violações com o objetivo de mitigar e prevenir danos desde o seu conhecimento.

7. Contração de Terceiros

O Diretor de Segurança Cibernética e da Informação poderá ainda contratar terceiro para prestar parecer técnico a fim de ser mapeado toda e qualquer vulnerabilidade, auxiliando-o no mapeamento dos riscos tecnológicos.

Respectiva nomeação visa adequar o Grupo Giant Steps às novas interações comerciais cada vez mais realizadas com a utilização de tecnologias e também manter-se em conformidade com as diretrizes estabelecidas pela Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais (ANBIMA) a fim de preservar prudentemente seus documentos digitais e dados sigilosos.

Previamente à contratação de qualquer serviço o Grupo Giant Steps irá se assegurar da capacidade funcional do fornecedor além do cumprimento a legislação vigente. Caberá também ao Grupo Giant Steps empreender seus melhores esforços para assegurar-se da confidencialidade, integridade e disponibilidade de recuperação de dados do fornecedor.

ANEXO I - Modelo de Relatório Anual de Segurança Cibernética e da Informação

São Paulo, _____ de março de 20XX.

Aos [●],

Ref.: Relatório Anual de Segurança Cibernética e da Informação

Prezados, Em vista do processo de reciclagem anual das regras, políticas, procedimentos e controles internos do GRUPO GIANT STEPS ("Gestora"), nos termos do Manual de Controles Internos (compliance) da Gestora ("Manual de Compliance"), e do Artigo 22 da Instrução nº 558, de 26 de março de 2015 da Comissão de Valores Mobiliários ("Instrução CVM 558"), e na qualidade de diretor responsável pela Segurança Cibernética e da Informação conforme dispõe o Manual de Compliance e seguindo as Diretrizes estabelecidas pela Comissão de Valores Mobiliários (CVM) e pela Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais (ANBIMA) , venho, nesta oportunidade, apresentar as seguintes considerações a respeito do período compreendido entre 1º de janeiro e 31 de dezembro de 20[--].

(i) A conclusão dos exames efetuados;

(ii) As recomendações a respeito de deficiências e cronogramas de saneamento;

(iii) Recomendações e Cronogramas de Saneamento; e

(iv) Minha manifestação, na qualidade de responsável pela Segurança Cibernética, a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las.

Fico à disposição para eventuais esclarecimentos que se fizerem necessários.

_____

Diretor de Segurança Cibernética e da Informação