HELIUS

CAPITAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

HELIUS CAPITAL GESTÃO DE RECURSOS S.A.

Agosto / 2021

APRESENTAÇÃO

A Política de Segurança da Informação da Helius Capital Gestão de Recursos Ltda. (“HELIUS”), aplica-se a todos os sócios, Colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da HELIUS, ou que HELIUS acesse informações a ela pertencentes. Todo e qualquer usuário de acessos computadorizados ou digitais da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

OBJETIVOS

A Política de Segurança da Informação da HELIUS visa proteger as informações de sua propriedade e/ou sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da HELIUS, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais relacionadas à empresa.

O Brasil aprovou em 2018 a Lei Geral de Proteção de Dados Pessoais (“LGPD”), a Lei nº 13.709/18, que assegura a proteção dos dados de titulares que sejam pessoas naturais. Importância da adequação das empresas à LGPD deve-se ao fato de que o fluxo de Dados Pessoais tratados deverá ser sistematizado e utilizado nos moldes da lei, permitindo que haja uma boa prática de privacidade perante seus clientes, aumentando o nível de confiança.

Qualquer informação sobre a HELIUS, ou de qualquer natureza relativa às atividades da empresa e a seus sócios, colaboradores 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 pelo Diretor de Riscos e *Compliance*.

SEGURANÇA DE INFORMAÇÕES

As medidas de segurança da informação utilizadas pela HELIUS têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis da HELIUS e circulem em ambientes externos à empresa com os mesmos, sem prévia autorização do Diretor de Riscos e *Compliance*. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais e/ou sensíveis. Cabe ressaltar que, em relação a informações de caráter sensível ou confidencial da empresa ou de clientes, estas serão armazenados em diretórios de rede com acesso restrito, e controlado pela equipe de Riscos e *Compliance* da HELIUS.

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 HELIUS. 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, manutenção de sua confidencialidade e descarte apropriado. Ainda, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da HELIUS.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. 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, sendo recomendável o seu descarte total. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pelo Diretor de Riscos e Compliance da HELIUS.

Adicionalmente, os Colaboradores devem se abster de utilizar *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios, físicos ou virtuais, que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na HELIUS.

É proibida a conexão de equipamentos na rede da HELIUS que não estejam previamente autorizados. Novos equipamentos e/ou sistemas deverão ter suas

configurações pela equipe de TI. Todo acesso a USB para armazenamento é bloqueado via *software* nos equipamentos.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (login de usuário) ao menos a cada três meses, utilizando modelo de definição de senha de difícil identificação por parte de potenciais "*hackers*" externos. Tal processo será auditável e rastreável eletronicamente baseado no sistema de *logon* do sevidor e serviços de informação.

O Colaborador pode ser responsabilizado 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.

O acesso a sites e *blogs*, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da HELIUS.

Programas instalados nos computadores, principalmente via internet (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia, além de avaliação de segurança pela empresa contratada para prover suporte de TI. Não é permitida a instalação de nenhum *software* ilegal ou que possuam direitos autorais protegidos, ou mesmo legal, sem prévia autorização do Diretor de Riscos e *Compliance*. Não é permitida a instalação de *software* nos equipamentos sendo restrito à equipe de tecnologia.

Também não é permitida a utilização de programas, sistemas e quaisquer plataformas virtuais, não autorizadas pelo Diretor de Riscos e *Compliance*, de alteração, guarda e transferência de arquivos.

Todo conteúdo que está na rede pode ser acessado pelos sócios ou pelo Diretor de Riscos e *Compliance* caso haja necessidade, inclusive e-mails. Arquivos pessoais

salvos em cada computador poderão ser acessados, caso seja necessário. A confidencialidade dessas informações deve ser respeitada, e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais, ou em atendimento a determinações judiciais ou administrativas. O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, a critério do responsável pela segurança cibernética.

Por fim, convém ressaltar que a HELIUS conta com sistemas e ferramentas contratados para arquivamento (rede), firewall, antivírus, backup, prevenção de invasão e linha de contingência.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 16 da Instrução CVM nº 558/15, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

SERVIÇOS DE REDE

As redes de serviços são segmentadas para garantia a segurança e desempenho entre elas. Está implantado um sistema de prevenção de invasão na rede e nos equipamentos para garantir a segurança da informação e disponibilidade de serviços.

TRATAMENTO DE DADOS

O Tratamento de Dados Pessoais será realizado observando a necessidade do fornecimento de Consentimento do Titular do dado e de realizar o cumprimento de obrigação legal ou regulatória pela Controladora.

Outras atividades que poderão ser realizadas no que tange ao Tratamento de dados se relacionam à realização da execução de contratos ou de procedimentos preliminares relacionados a contrato do qual o Titular do dado seja parte, ao exercício regular de direitos em processos judiciais, administrativos ou arbitrais, a proteção da vida ou da incolumidade física do Titular ou de terceiros, em atendimento aos interesses legítimos

da Controladora ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos Dados Pessoais, além de se relacionar com a proteção de crédito.

Cabe ressaltar que a HELIUS ao obter o Consentimento do Titular do dado para realizar o Tratamento do mesmo deve, caso aplicável, também, obter Consentimento específico do próprio Titular para comunicar ou compartilhar Dados Pessoais com outros controladores ou Operadores. O Consentimento do Titular deverá ser fornecido por meio que demonstre a manifestação de vontade do Titular.

O Consentimento poderá ser revogado pelo Titular do Dado Pessoal, para que não tenha mais seus dados tratados, a qualquer momento por meio da manifestação expressa do Titular, por procedimento gratuito e garantindo que possa haver a exclusão dos dados tratados.

É direito do Titular dos dados ter acesso facilitado às informações relativas ao Tratamento de seus dados disponibilizados, podendo requisitar a existência e o acesso aos seus dados a qualquer momento. Além disso, resta assegurado que ao término do Tratamento de Dados Pessoais, eles serão eliminados, sendo apenas conservados para o cumprimento de obrigação legal ou regulatória pela HELIUS, estudo de órgão de pesquisa, transferência a terceiro e uso exclusivo da Controladora, sendo vedado acesso por terceiro.

Os Agentes de Tratamento de Dados Pessoais devem manter os registros referentes ao Tratamento de Dados Pessoais que realizarem. Nesse sentido, a ANPD poderá determinar e requerer que a Controladora elabore um relatório de impacto à proteção de Dados Pessoais, inclusive de dados sensíveis.

Será de responsabilidade da Controladora e do Operador, em razão da atividade de Tratamento de Dados Pessoais, ressarcir os danos que causarem relacionados ao dano patrimonial, moral, individual ou coletivo, em violação à legislação.

A nossa Política de Privacidade, abaixo, esclarece como a HELIUS coleta e trata seus dados individuais:

1. Todas os Dados Pessoais fornecidos pelo usuário, bem como aquelas que são geradas automaticamente, como as características do dispositivo de acesso, protocolo de internet (“IP”), informações de acessos, dados de geolocalização, histórico de aplicações e dados informados para o login, são recebidas e armazenadas em ambiente seguro, no Banco de Dados da HELIUS;

2. Todas as informações coletadas dos usuários trafegam de forma segura, utilizando processo de criptografia padrão da Internet;

3. Os Dados Pessoais que nos forem fornecidos pelos usuários serão coletadas por meios éticos e legais;

4. Os usuários serão avisados que os seus Dados Pessoais estão sendo coletados, ficando a seu critério fornecê-los ou não, e serão informados também sobre as consequências de sua decisão;

5. A menos que tenhamos determinação legal ou judicial, as informações dos usuários jamais serão transferidas a terceiros ou usadas para finalidades diferentes daquelas para as quais foram coletadas;

6. O acesso aos Dados Pessoais coletados é restrito aos profissionais autorizados e qualificados que necessitem das mesmas exclusivamente para o desempenho de suas funções;

7. Os funcionários que se utilizarem indevidamente dessas informações, ferindo nossa Política de Privacidade, estarão sujeitos às penalidades previstas em nosso processo disciplinar, inclusive desligamento por justa causa, não excluindo eventual responsabilização civil ou penal;

8. Manteremos a integridade das informações que nos forem fornecidas;

9. Nosso site pode conter links para outros sites externos, cujos conteúdos e políticas de privacidade não são de responsabilidade da HELIUS;

10.Será exigida de toda organização contratada para prover serviços de apoio, o cumprimento aos nossos padrões de privacidade e segurança da informação;

11.Para fins de operações e gerenciamento de riscos, poderemos trocar informações sobre nossos clientes com fontes respeitáveis de referência, órgãos reguladores e serviços de compensação;

12.A HELIUS excluirá as informações coletadas quando: (i) a finalidade para a qual a informação foi coletada seja alcançada ou quando os dados deixarem de ser necessários ou pertinentes para o alcance desta finalidade, conforme finalidades descritas nos presentes Termos; (ii) quando da revogação do Consentimento, pelo usuário, nos casos em que este se fizer necessário; ou (iii) mediante determinação de autoridade competente para tanto.

13.A HELIUS pode coletar informações sobre as maneiras como os usuários acessam este site, transferindo um pequeno arquivo de texto conhecido como "cookie" para os dispositivos dos usuários. Essas informações por si só não identificam nenhum indivíduo e são usadas pela HELIUS para aprimorar a experiência do usuário neste site. Os usuários podem recusar cookies alterando as configurações do navegador, embora isso possa afetar adversamente a forma como eles experimentam este site.

Como essa política está sujeita a eventuais atualizações devido ao nosso compromisso com a melhoria contínua, recomendamos que seja consultada periodicamente. Na medida do aplicável, a HELIUS controla e processa todos os Dados Pessoais de acordo com os princípios da Lei n° 13.709, de 2008, Lei Geral de Proteção de Dados Pessoais, que dá aos usuários certos direitos, incluindo o de acessar as informações mantidas sobre eles e solicitar que essas informações não sejam usadas para um propósito específico. Tais direitos podem ser exercidos mediante contato com compliance@heliuscapital.com.br. Por esse mesmo endereço eletrônico, o Titular dos dados poderá solicitar uma cópia dos seus dados armazenados e tratados, a alteração ou correção de alguma informação ou a sua exclusão, pela HELIUS.

ARMAZENAMENTO DE DADOS

Todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas em serviços de armazenamento de dados na nuvem, cujo acesso é permitido apenas aos administradores da HELIUS e membros do departamento de tecnologia da informação.

O armazenamento de dados (*backup*) é realizado diariamente em *cloud* e localmente sendo disponível para *restore* após liberação do responsável de segurança da informação.

A HELIUS adota também backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de continuidade dos negócios da HELIUS.

Caso o Titular do dado seja um cliente ativo, seus dados serão mantidos enquanto durar a relação contratual ou comercial. Assim, a HELIUS poderá armazenar seus Dados Pessoais em um Banco de Dados para eventual cumprimento legal, por 5 (cinco) anos após o término da relação contratual ou comercial.

Caso o Titular do dado seja um cliente em potencial sem relação contratual ou comercial, específico, não serão mantidos seus Dados Pessoais por mais de 3 (três) anos após sua última consulta.

Caso o Titular do dado seja um candidato e não for contratado, as informações compartilhadas serão excluídas em até 2 (anos) após seu compartilhamento, do Banco de Dados da HELIUS.

COMPARTILHAMENTO DE DADOS

Os dados armazenados e tratados pela HELIUS podem ser compartilhados com parceiros comerciais que realizem atividades terceirizadas com a finalidade de cumprir com o negócio firmado entre o Titular do dado e a HELIUS.

Eventualmente, a HELIUS poderá ser obrigada a divulgar informações pessoais, por lei, processos legais, litígios ou solicitações de Autoridades Públicas e Governamentais, seja para fins de segurança nacional, aplicação de lei ou outras questões de importância pública.

INSTALAÇÕES FÍSICAS TECNOLOGIA / ACESSO FÍSICO.

Para garantir o ambiente em alta disponibilidade está implantado um nobreak central para assegurar problemas de energia. O sistema de ar condicionado está implantado

no CPD. O acesso físico ao CPD é controlado e autorizado somente pessoas da equipe de tecnologia da informação ou afins.

INDISPONIBILIDADE DE ACESSO À INFORMAÇÃO

Em caso de problemas de indisponibilidade de acesso à informação é acionado o processo de plano crises sendo avaliado o impacto sobre o negócio.

PLANO DE IDENTIFICAÇÃO E RESPOSTA A INCIDENTES

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da HELIUS (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser prontamente informada ao Diretor de Riscos e *Compliance.* O Diretor de Riscos e *Compliance* determinará quais membros da administração da HELIUS e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Riscos e *Compliance* determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

- Procedimentos de Resposta

O Diretor de Riscos e *Compliance* responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da HELIUS de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais

serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da HELIUS, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

(vii) Determinação do responsável (ou seja, a HELIUS ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Riscos e *Compliance*, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES

A HELIUS entende essencial que o seu treinamento anual, supervisionado pelo Diretor de Riscos e *Compliance*, abranja todos os preceitos contidos na presente política, de modo que seus Colaboradores estejam sempre cientes e consonantes os procedimentos de segregação e segurança das informações.

RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES

Anualmente, a HELIUS realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos Colaboradores, individualização dos usuários, dentre outros.

Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão descritos no Relatório Anual de Controles Internos da HELIUS.

Estes testes serão realizados pela equipe de suporte de TI contratada, e buscará cobrir os seguintes pontos:

- Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de *hardware* e *software*, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;
- Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;
- Detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;
- Validação da eficiência do plano de resposta e recuperação de incidentes;
- Manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas em diretório interno da área de Riscos e Compliance como evidência em eventuais questionamentos internos ou de órgãos reguladores ou autorreguladores.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê Trimestral de Riscos e *Compliance*, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada semestralmente, 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.