AheadVentures

Política de Segurança da Informação e Segurança Cibernética

1. Introdução

1.1. A Política de Segurança da Informação e Segurança Cibernética ("Política") da **Ahead Ventures Gestão de Recursos e Consultoria Ltda**., denominada neste documento "**Ahead**" ou "**Gestora**", visa preservar a confidencialidade, integridade e disponibilidade das informações no desempenho de suas atividades, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte, bem como estabelecer regras para acesso físico às instalações da Ahead.

1.2. Esta Política foi desenvolvida em atenção aos dispositivos da Resolução CVM nº 21/2021 ("Res. CVM 21") e do Código ANBIMA de Administração de Recursos de Terceiros ("Código") e do Guia ANBIMA de Cibersegurança ("Guia").

2. Abrangência e Atualizações

2.1. Esta Política de Segurança da Informação e Segurança Cibernética tem como público-alvo todos os usuários da Ahead, seja os diretores, colaboradores e/ou prestadores de serviços, que possuem acessos a dependências da gestora e/ou que tenham acesso a qualquer tipo de ativo de informação que pertença ou que estejam sob a responsabilidade da Ahead.

2.2. Política de Segurança da Informação e Segurança Cibernética será atualizada em prazo não superior a 24 (vinte e quatro) meses, ou quando houver alteração na Regulação que demande modificações.

3. Acessibilidade

3.1. A Política de Segurança da Informação e Segurança Cibernética, tem a finalidade de minimizar as ameaças aos negócios da Ahead e às disposições desta Política, quanto a normas e procedimentos relativos ao tratamento dos ativos de informação e/ou dados sigilosos a serem apresentados aos usuários, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento.
3.2. A presente Política está disponível na nuvem da Ahead, em um diretório disponibilizado pelo Compliance para a consulta a todos os usuários da gestora.

4. Responsabilidade

4.1. A Ahead se utiliza de um prestador de serviço , empresa terceira contratada para administrar a sua área de Tecnologia da Informação - TI, é de responsabilidade da Diretoria de Compliance o gerenciamento e controle de qualidade do serviço prestado por este.

5. Diretrizes de Segurança da Informação e Segurança Cibernética

5.1. A Segurança da Informação nada mais é que um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os usuários, visando à proteção adequada dos que compartilham a informação. Define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável.

5.2. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo. Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas ao nosso meio.

5.3. Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irretratabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

5.4. Dessa forma, os princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

5.5. Assim, a Ahead preserva suas informações quanto a:

(i) **Confidencialidade:** Garantir que as informações sejam acessadas apenas por pessoas autorizadas;

(ii) **Integridade:** Garantir que as informações, tanto em sistemas quanto em bancos de dados, estejam em um formato verdadeiro e correto para seus propósitos originais;

(iii) **Disponibilidade:** Garantir que as informações e os recursos estejam disponíveis para aqueles que precisam delas quando necessário;

(iv) **Acesso Controlado:** O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede;

(v) **Finalidade:** independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada;

(vi) **Necessidade:** garantir que cada Colaborador tenha acesso exclusivamente às informações necessárias ao desempenho de suas atribuições.

5.6. A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo

o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos. A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger a rede, os computadores, os sistemas e os dados de ataques ou acessos não autorizados.

5.7. O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

5.8. Há diversas razões para que esses ataques ocorram e os principais motivos são:

(i) obter recursos financeiros;
(ii) roubar e manipular informações;
(iii) obter informações privilegiadas;
(iv) sabotagem à instituição;
(v) disseminar falsas notícias; e
(vi) disseminar o caos.

5.9. A segurança cibernética deve garantir:

(i) a segurança dos sistemas e dos bancos de dados;
(ii) o gerenciamento das pessoas autorizadas;
(iii) a segurança dos sistemas e informações que estão na nuvem;
(iv) a segurança para todos os dispositivos/equipamentos;
(v) o planejamento da continuidade do negócio; e
(vi) o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

5.10. São exemplos de consequências/danos que podem ser causados pela falha na segurança cibernética:

(i) risco de imagem;
(ii) risco de continuidade do negócio; e
(iii) prejuízos financeiros.

6. Identificação e Avaliação de Riscos

6.1. A Ahead conta com um servidor de processamento de dados e armazenamento em nuvem da Microsoft OneDrive e computadores individuais para todos os seus colaboradores para executar todas as suas funções. É possível armazenar e hospedar qualquer arquivo, usando uma Conta da Microsoft, bem como, é possível definir arquivos públicos, somente em grupos restritos, usuários definidos ou privados.

6.2. No âmbito de suas atividades, a Ahead identificou os seguintes principais riscos internos e externos que precisam de proteção:

(i) **Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de investidores, parceiros, prestadores de serviços, Colaboradores e dados da Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

(ii) **Sistemas:** informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

(iii) **Processos e Controles:** processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e

(iv) **Governança da Gestão de Risco:** a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

6.3. Nesse contexto, para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para Gestora, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Ahead, em caso de incidente de segurança.

6.4. Ademais, no que se refere especificamente à segurança cibernética, a Ahead identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

(i) **Malware**: softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);

(ii) **Engenharia social:** métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

(iii) **Ataques de DDoS (distributed denial of services) e botnets:** ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

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

6.5. Com base no acima, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

7. Ações de Prevenção e Proteção

7.1. No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, ficam armazenadas em serviços de armazenamento de dados, cujo acesso é permitido, além dos membros do departamento de informática, a qualquer usuário sob autorização do departamento de Compliance.

7.2. Todo software disponibilizado pela área de TI da Ahead, autorizados pelo Compliance, deverá ser utilizado somente para os negócios da Gestora, em consonância com os acordos de licenciamento firmados.

7.3. É realizado backup de todas as informações e armazenadas em nuvem, de acordo com as diretrizes do OneDrive da Microsoft, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

7.4. O acesso aos sistemas de informação da Ahead é feito por meio de um par "usuário/senha" que permite ao departamento de informática acompanhar, de forma precisa as atividades desenvolvidas por cada um dos colaboradores. O controle desses dados é de domínio da Gestora, uma vez que o armazenamento dos dados ocorre no servidor em nuvem da Microsoft, garantindo, assim, a confidencialidade e confiabilidade da informação.

7.5. Todos os acessos concedidos são avaliados conforme o envolvimento de cada usuário com a Ahead. Desta forma, a concessão de acesso às informações obtidas, será considerado o exercício da atividade desempenhada e a respectiva área (quando aplicável) de forma restrita e limitada ao usuário de acordo com o tipo de vínculo, que o usuário terá com a Ahead. Para tanto, serão criados diretórios específicos, a partir dos quais será possível controlar a concessão de acessos de acordo com as regras estabelecidas.

7.6. Todo usuário que tiver acesso aos sistemas de informação da Ahead é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O usuário deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não divulgá-los a terceiros em qualquer hipótese.

7.7. Todos os usuários deverão respeitar a regras estabelecidas nos termos da presente Política e do Código de Conduta e Conduta da Gestora. Para isto, cada usuário que tiver acesso a nuvem da Ahead, deverá firmar o Termo de Acesso de Rede Corporativa OneDrive ("Termo"), conforme descrito no "Anexo I" desta Política, atestando expressamente seu conhecimento, comprometendo-se a cumprir as regras determinadas.

8. Regras para uso de Tecnologia

8.1. Internet: Todos os usuários da Ahead têm o dever de utilizar a internet exclusivamente para assuntos relacionados aos negócios conduzidos pela Gestora ou para o desempenho de suas atividades, sendo de sua inteira responsabilidade, o uso estritamente profissional,

8.2. Aplicativos de Mensagens: Todos os usuários da Ahead têm o dever de utilizar os aplicativos de mensagens exclusivamente para assuntos relacionados aos negócios conduzidos pela Gestora ou para o desempenho de suas atividades.

8.3. Mídias externas e/ou portáteis: Todos os sócios e colaboradores da Ahead são proibidos de utilizar mídias externas e/ou portáteis para transferir dados, sistemas e arquivos da rede da Gestora.

8.4. Correio Eletrônico: A utilização da internet por nossos colaboradores deve ter como finalidade profissional. Os usuários da gestora têm uma conta de e-mail em seu nome sendo esta, de sua inteira responsabilidade, devendo ser utilizada de acordo com as normas de conduta ética e de segurança do Ahead, sendo sua utilização estritamente profissional.

8.5. Trabalho Híbrido: A Ahead realiza sua jornada de trabalho no formato de trabalho híbrido, desse modo, todos os computadores serão adaptados a esta modalidade. Ademais, a Ahead possui um controle adequado que prevê os acessos locais ou remotos a ativos também locais ou remotos e prever a possibilidade de uso de dispositivos pessoais nesses casos (Bring Your Own Device - BYOD).

8.6. Utilização de recursos: Todos os usuários da Ahead têm o dever de não utilizar os recursos disponibilizados pela Ahead como de uso pessoal.

8.7. Compartilhamento de Dados e Processamento, Armazenamento de Dados, Backup e Computação em Nuvem: Não é permitido o compartilhamento de pastas nos computadores e desktops da Ahead sem autorização prévia. Todos os dados deverão ser armazenados em rede/nuvem, e a autorização para acessá-los deverá ser fornecida pelo Compliance. O Backup é realizado em nuvem OneDrive é realizado diariamente de forma automática.

8.8. Uso de Senhas: As senhas são únicas, pessoais e intrasferíveis e tornam o portador da senha responsável por todas as ações praticadas, inclusive se utilizadas por terceiros. O compartilhamento de senhas, em quaisquer hipóteses, é expressamente proibido. As

senhas deverão ser trocadas, conforme aviso fornecido pelo sistema/software utilizado. Como melhores práticas poderão ser trocadas anualmente.

8.9. Firewall, Software, Varreduras (Antivírus): A Ahead mantém proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, worms, spyware). Essa proteção é realizada pelo antivírus TrendMicro Maximum Security. Serão conduzidas varreduras diárias e mensais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Gestora. A gestora utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches.

8.10. Destruição de Documentos: 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 ou leitura.

8.11. Monitoramento: Conforme mencionado neste capítulo, a utilização dos recursos disponibilizados pela Ahead está sujeita ao monitoramento periódico, sem frequência determinada ou aviso prévio. Adicionalmente, os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto desta Política e demais regras internas da Gestora, e, conforme o caso servir como evidência em processos administrativos e/ou legais.

8.12. Controle de Acesso: O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa do Compliance. Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, sendo permitido o seu uso para fins pessoais de forma moderada, como ferramenta para o desempenho de suas atividades.

8.13. Utilização de Aplicativos: Não é recomendado o tráfego de qualquer tipo de documentos e informações pertinentes para a Ahead, compartilhados via aplicativos tais

como: redes sociais, WhatsApp, bate papos, etc., sem autorização da Diretoria da Ahead. É recomendado a utilização do e-mail e o Microsoft Teams corporativo da Gestora para essa funcionalidade.

9. Testes Periódicos

9.1. Periodicamente, a Ahead realiza testes de segurança em todo o seu sistema de informação, de forma a garantir, as ações de prevenção e proteção.

10. Criação de um Plano de Resposta

10.1. No caso de um eventual ciberataque, o procedimento a ser adotado depende do grau de severidade do ataque sofrido:

(i) Utilização comprometida de um ou mais computadores: Os usuários afetados têm o dever de reportar o problema para a Diretoria de Compliance e área de tecnologia da informação. Nesse caso, a área de tecnologia da informação tem o dever de tentar reparar o prejuízo causado ao usuário prejudicado; e

(ii) Utilização comprometida de todo o servidor nuvem e/ou de todos os computadores: os usuários afetados têm o dever de reportar o problema para a Diretoria de Compliance e a área de tecnologia da informação. Nesse caso, a área de tecnologia da informação tem o dever de tentar reparar o prejuízo causado e a Política de Contingência: Plano de Continuidade de Negócios é acionada.

11. Reciclagem e Revisão

11.1. A Diretoria de Compliance em conjunto com a área de tecnologia da informação, ficam incumbidas de produzirem um relatório toda vez que cibersegurança da Ahead for comprometida. Esse relatório é apresentado no Comitê de Risco, Compliance e PLD e contempla os danos incorridos e as ações tomadas e sugestões para melhora com relação ao procedimento.

12. Arquivamento de Informações

12.1. De acordo com o disposto nesta Política, os usuários deverão manter arquivada toda e qualquer informação, 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.

13. Considerações Finais

13.1. Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com o Compliance da Ahead.

14. Manutenção dos Arquivos

14.1. A Ahead manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Compliance desta Política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

AheadVentures

TERMO DE ACESSO A REDE CORPORATIVA ONEDRIVE

Considerando que (i) a **AHEAD VENTURES GESTÃO DE RECURSOS E CONSULTORIA LTDA**, inscrita no CNPJ nº 44.206.305/0001-20, neste ato doravante designada "**AHEAD VENTURES**", e (ii) Razão Social/Nome, inscrita no CNPJ/CPF nº XXXXXX, neste ato doravante designada "**USUÁRIO**".

A fim de garantir a proteção e preservação do sigilo das informações contidas em sua rede interna corporativa, disponibilizada via OneDrive da Microsoft pela **AHEAD VENTURES**, com acesso designado a uma pasta específica, considerado uma ferramenta institucional para armazenamento em nuvem, com a possibilidade de armazenar, compartilhar e sincronizar qualquer arquivo.

Sendo assim, nos termos do Código de Ética e Conduta da **AHEAD VENTURES** e demais políticas aplicáveis, na qualidade de **USUÁRIO**, declaro ter acesso à rede interna corporativa da **AHED VENTURES**, segregada via OneDrive, e me comprometo a:

i. Acessar a rede corporativa, somente com autorização, por necessidade de serviço ou por determinação expressa de algum superior hierárquico;
ii. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, sendo as informações contidas nas pastas consideradas como sigilosas;
iii. Comprometo-me a zelar pelo uso profissional e correto da pasta, em absoluto sigilo das informações contidas, como também, a solicitar o cancelamento de acesso caso ocorra qualquer alteração da representatividade legal que hoje detenho;
iv. Não me ausentar da estação de trabalho sem bloquear a estação de trabalho, bem como encerrar a o usa da pasta corporativa, garantindo assim a impossibilidade de acesso indevido por terceiros;
v. Respeitar as normas de segurança e restrições impostas e implantados pela AHEAD VENTURES a fim de garantir a segurança da informação;

vi. Responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de acesso a pasta e/ou diretório restrito;
vii. De forma geral, sempre que houver a coleta de informações relacionadas à pessoa física, essas informações serão consideradas Dados Pessoais para fins da legislação de proteção de dados, a LGPD, a Lei 13.709/18 e redações dadas pela Lei nº 13.853/19);
viii. Respeitar e acatar todas as cláusulas constantes neste termo; e
ix. Cumprir as determinações que constam na Política de Segurança da Informação da AHEAD VENTURES.

São vedados ao usuário:

i. Armazenar no servidor em nuvem qualquer informação, dado ou material que viole qualquer Lei;
ii. Armazenar no servidor qualquer informação instrutiva sobre atividades ilegais, que promovam ou induzam dano físico ou moral contra qualquer grupo ou indivíduo;
iii. Armazenar no servidor qualquer material de cunho racista, neonazista, antissemita ou qualquer outro que venha a atentar contra a integridade moral de terceiros ou grupos da sociedade; e
iv. Armazenar no servidor qualquer material de cunho erótico ou pornográfico.

O usuário assumirá a responsabilidade por dano causado por algum procedimento de iniciativa própria de tentativa de modificação da configuração, física ou lógica, da nuvem disponibilizada sem a autorização expressa.

O usuário assumirá a responsabilidade pelo dano que possa causar caso não venha a cumprir o disposto neste termo.

Cada parte deverá atuar em conformidade e confidencialidade com a legislação vigente com as determinações de órgãos reguladores/fiscalizadores sobre a matéria.

AheadVentures

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plenamente e integralmente.

XXX, XX de XX de 2023.

_____

Usuário: XXXXXXXXX