POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

1. OBJETIVO

A política de segurança da informação e segurança cibernética ("Política de Segurança da Informação") dispõe sobre à recepção, armazenamento e utilização das informações corporativas e pessoais disponibilizadas aos Colaboradores, conforme definido abaixo, da Augme Capital Gestão de Recursos Ltda. ("Augme").

A Política de Segurança da Informação leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Augme.

A coordenação direta das atividades relacionadas à Política de Segurança ficará a cargo do Diretor de Risco, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme descrito no Manual.

2. ABRANGÊNCIA

Esta Política de Segurança deve ser seguida por todos os sócios diretos ou indiretos, diretores, funcionários, estagiários e prestadores de serviço, se aplicável, da Augme (doravante designado como o "Colaborador" e em conjunto como os "Colaboradores").

3. PRINCÍPIOS

Essa Política tem como objetivo definir os princípios e diretrizes que visam a preservação da segurança da informação, primando pela confidencialidade, integridade e disponibilidade.

A Augme pode alterar a qualquer momento, a seu exclusivo critério, os termos e condições da Política de Segurança, sendo obrigatória sua verificação periódica.

3.1. Objetivos da Segurança da Informação

Confidencialidade: Garantir que as Informações Confidenciais (conforme definidas no Manual de Conduta e Ética) tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: Garantir que as informações sejam mantidas íntegras, sem modificações indevidas, seja acidental ou proposital;

Disponibilidade: Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

3.2. Importância da Segurança da Informação

3.2.1. Riscos

A Augme está em risco quando não são respeitados quaisquer de seus objetivos de Segurança da Informação.

3.2.2. Vulnerabilidade

É uma falha ou um ponto fraco no desenvolvimento, na implantação ou no uso da informação. Essa falha ou ponto fraco pode ser explorado, intencionalmente ou não, para reduzir a segurança através da não observância de seus objetivos básicos: Confidencialidade, Integridade e Disponibilidade.

As vulnerabilidades relativas a processo e sistemas, uma vez conhecidas, podem ser exploradas em prejuízo da instituição, a qualquer tempo.

3.2.3. Incidente de Segurança

É um evento ocorrido que viola a Segurança da Informação. Trata-se da exploração das vulnerabilidades em processos ou sistemas. Os incidentes, intencionais ou não, ocasionam a perda de qualidade da informação.

Quando tiver suspeitas ou conhecimento de ocorrências de atividades que prejudiquem as operações da Augme, o Colaborador não deve hesitar em informar imediatamente o diretor responsável e à equipe de Segurança da Informação.

3.3. Identificação de Riscos (*risk assessment*)

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

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Augme, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pela Augme e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Augme;
- Governança da Gestão de Risco: a eficácia da gestão de risco pela Augme quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

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

- Malware – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware, e Ransomware);
- Engenharia social – métodos de manipulação para obter Informações Confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);
- Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- Invasões (advanced persistent threats): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no disposto acima, a Augme 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.

3.4. Ações de Prevenção e Proteção

Após a identificação dos riscos, a Augme adota as medidas a seguir descritas para proteger suas informações e sistemas.

3.4.1. Uso interno da Informação Confidencial

- Informações Confidenciais são de uso restrito a Colaboradores, e não devem ser divulgadas a terceiros;
- Este tipo de informação inclui atividades, processos e material exclusivo da instituição que, uma vez divulgados ao público em geral provocará danos em pequena ou grande escala;
- Informações de uso interno exigem esforços adequados de segurança, visando evitar perdas, e atenção concentrada em garantir a Integridade e Disponibilidade.

3.4.2. Ciclo de vida da Informação Confidencial

Toda Informação Confidencial possui um ciclo de vida composto pelas seguintes fases:

- Cópia e Transferência da Informação Confidencial
- Guarda
- Uso
- Transferência
- Destruição

3.4.2.1. Cópia e Transferência da Informação Confidencial

Cópias de Informações Confidenciais devem ser feitas com autorização explícita do proprietário ou geradas da informação e controlada por ele. A atenção deve ser redobrada para arquivos eletrônicos, uma vez que sua cópia e distribuição são facilitadas;

Quando for necessário transferir Informações Confidenciais, prefira que seja pessoalmente ou através da utilização de serviço de entrega autorizado e confiável;

O Colaborador deve sempre registrar as informações básicas dos destinatários da Informação Confidencial: Nome, local, empresa e número de documento.

Lacre envelopes contendo o Informação Confidencial e escreva a palavra "confidencial" no envelope.

O Colaborador deve tomar cuidado para não revelar Informações Confidenciais em ambiente público, dentro ou fora da Augme.

A Augme realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Augme e circulem em ambientes externos à Augme com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como Informações Confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito por qualquer dos membros do Comitê de *Compliance*.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Augme. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a Informação Confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Colaboradores deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a área de *Compliance* deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Augme qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Em consonância com as normas internas acima, os Colaboradores apenas podem utilizar pen-drivers ou quaisquer outros meios após obter autorização e aprovação formal com sua gerência, sendo certo que é vedado a utilização que não tenha por finalidade a utilização exclusiva para o desempenho de sua atividade na Augme.

3.4.2.2. Acesso Escalonado ao Sistema

A Augme mantém diferentes níveis de acesso a pastas e arquivos eletrônicos, notadamente aqueles que contemplem Informações Confidenciais, de acordo com as funções e responsabilidades dos Colaboradores e pode monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e login disponibilizados.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Augme em caso de violação.

3.4.2.3. Guarda da Informação Confidencial

Para que se mantenha confidencial, a informação dependerá que seu proprietário realize a guarda de maneira correta.

- Mantenha a informação em local seguro, trancado e sem acesso público;
- Evite revelar os locais de armazenamento e os motivos de guardar as informações neste local, dificultando acesso ao material confidencial por pessoas não autorizadas;
- Se a Informação Confidencial for eletrônica, se utilize de meios seguros para armazená-las;
- Se estiver em notebooks ou outros dispositivos móveis, tenha atenção redobrada ao equipamento – um dos alvos mais visados em assaltos e furtos;
- Nunca deixe papéis e arquivos confidenciais em impressoras ou cestas de lixo, anotações em quadro branco, arquivos em computadores de uso comum utilizados em apresentações.

3.4.2.4. Uso da Informação Confidencial

As informações devem ser usadas de modo racional, evitando ser expostas a riscos desnecessários.

- Retire o material de seu local de armazenamento apenas quando for necessário;
- Nunca deixe senhas e outras formas de acesso próximas a seu local de trabalho.

3.4.2.5. Destruição da Informação Confidencial

Cópias da Informação Confidencial em número excessivo ou exemplares desnecessários devem ser destruídos corretamente, evitando riscos de disseminação da informação:

- Material físico deve ser destruído utilizando-se trituradores de documentos.
- No caso de material eletrônico, destrua as mídias. Se for necessário reaproveitá-las, utilize programas especialmente desenvolvidos para apagar todas as trilhas da mídia.

No caso de perda ou Roubo da Informação Confidencial, avise o Diretor de *Compliance/PLDFT* para avaliação dos impactos, danos ou riscos e a definição do plano de ação.

3.5. Utilização de equipamentos e sistemas

Computadores, redes e sistemas da instituição são recursos disponíveis ao Colaborador para atividades de sua função.

Equipamentos pessoais de Colaboradores, como computadores móveis, smartphones e mídias de armazenamento removível, dentre outros, não podem ser utilizadas para guarda ou transferência de informações confidenciais da Augme.

A utilização dos ativos e sistemas da Augme, incluindo computadores, telefones, internet, e-mail, plataformas aprovadas pelo *Compliance* para transmitir mensagens instantâneas (Microsoft teams) e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o fato a qualquer dos membros do Comitê de *Compliance*.

Todas as informações contidas nos equipamentos e sistemas da Augme são de propriedade da empresa.

Mesmo prezando pela privacidade de cada Colaborador, alguns procedimentos investigativos que precisem ser instaurados para manter os interesses da organização ou por determinação judicial, podem requerer rastreamento e verificação de documentos e sistemas. Portanto, recomenda-se evitar manter arquivos pessoais armazenados nos recursos da empresa, mesmo sendo permitida a utilização desses recursos para atividades pessoais, desde que não influenciem negativamente nas finalidades de negócio da organização e no exercício de suas funções.

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

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da Augme.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, gênero, orientação sexual ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.
Cada Colaborador é responsável, ainda, por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

3.6. Uso de senhas

As senhas de acesso devem ser dadas a mesma importância que damos a outras senhas utilizadas em nosso cotidiano. A Augme se utiliza de meios de controle para garantir a utilização segura de senhas.

Cuidados especiais:

- Nunca divulgue ou compartilhe sua senha com outras pessoas;
- Evite reutilizar senhas antigas;
- Não anote sua senha em um arquivo de computador ou em um papel que possa cair em mãos de uma pessoa não autorizada;
- Ao digitar sua senha, certifique-se que ninguém está observando enquanto você digita o teclado; e
- Altere sua senha todas as vezes que suspeitar que ela foi descoberta por alguém.

As senhas de acesso dos Colaboradores são parametrizadas e deverão ser alteradas a cada 6 meses. Caso, por qualquer, motivo, se verifique que os Colaboradores não estão alterando as senhas na periodicidade acima mencionada, os mesmos estarão sujeitos às sanções previstas nesta Política.

Adicionalmente, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

3.7. Mesa Limpa

Informações em papel deixadas sobre mesas e em armários de acesso público podem comprometer a segurança e permitir a perda de sua confidencialidade.

Sempre que se ausentar da estação de trabalho, o usuário é orientado a efetuar a bloquear seu computador com senha. Se sua ausência for prolongada, desligue a estação.

3.8. Utilização de Internet e correio eletrônico

A Augme oferece acessos à Internet e ao correio eletrônico a seus Colaboradores, de maneira que possam exercer suas atividades com eficiência. Estes recursos devem ser utilizados considerando os princípios corporativos de responsabilidade, respeito e profissionalismo.

A conexão da instituição à Internet está sujeita a diversos riscos, inerentes a esse processo. Portanto, cada usuário deve estar consciente de que sua estação de trabalho, possuindo este tipo de acesso, também tem sua parcela de contribuição para manter o nível de segurança da organização. Dê especial atenção aos tipos de sites em que navega na Internet e, também, às mensagens eletrônicas que envia, uma vez que todas as ações que realizamos, fazemos em nome da Augme.

A utilização para fins pessoais é permitida desde que não comprometa os interesses da organização ou sua produtividade no exercício de suas funções e, também, não incorra em custos adicionais da Augme.

Recomendações da Augme:

- Não acesse sites ou arquivos, tampouco responda ou envie mensagens eletrônicas de conteúdo que possa afetar a moral pessoal e da organização;

- Não envie mensagens ou acesse sites que afetem a produtividade de sua função;
- Verifique as opções de segurança disponíveis no site visitado. Evite sites que exigem informações confidenciais, senhas, sem oferecer garantia de transmissão de segurança;
- Antes de responder ou enviar uma mensagem, verifique o nome do remetente e destinatário. Tenha especial cuidado com mensagens de conteúdo confidencial para que não sejam enviadas para destinatários indevidos;
- Não leia mensagens de origem desconhecidas, com nome de remetentes ou títulos estranhos. Apague-as imediatamente;
- Não execute programas ou abra arquivos que não são esperados, mesmo que sejam provenientes de origem conhecida ou aparentemente inofensivos;
- Não envie mensagens contendo anexos que não foram incluídos intencionalmente por você. Fique atento à sua estação de trabalho e avise a área de Segurança da Informação e ao seu gestor quando houve suspeitas de infecção de vírus.

3.9. Utilização de computação móvel

A atenção para computador móvel deve ser redobrada, principalmente quando transportado.

Recomendações da Augme:

- Procure utilizar cofres em hotéis e outros lugares seguros;
- Não abandone o equipamento dentro de veículos e trate-o como equipamento sensível quando fizer viagens aéreas, carregando-o como bagagem de mão;
- Evite aparentar que transporta um notebook e outros recursos em locais públicos;
- Se for utilizar o equipamento internamente, tranque-o quando estiver longe de seu lugar de trabalho;
- Evite armazenar informações confidenciais no equipamento móvel e sempre utilize software de segurança especial para proteger o equipamento.

3.10. Utilização de Programas de Mensagens Instantâneas

A utilização de programas de “mensagens instantâneas” pode prejudicar a segurança da informação da instituição por ser uma ferramenta que facilita o envio e recebimento de dados, informações e documentos por vezes não autorizados. Além disso, a empresa fica mais exposta ao recebimento de vírus que podem causar a perda parcial ou total do equipamento.

É proibido o uso destes programas que não tenham objetivo profissional. A instituição neste caso se reserva ao direito de monitorar e gravar as conversas dos funcionários evitando a evasão de informações estratégicas.

3.11. Wireless

A Augme disponibiliza acesso a uma rede Wireless que está separada da rede local, esta rede fornece aos Colaboradores acesso à internet. Para ter este acesso à internet por meio deste dispositivo o Colaborador deve solicitar a senha com a área de Segurança da Informação.

A rede wireless para acesso à internet disponibilizada pela Augme é criptografada e protegida por senha, seguindo as boas práticas de segurança.

3.12. Dispositivos Removíveis

Caso necessário à utilização de mídias de armazenamento como *pendrive* e dispositivos similares para transporte de informações da organização, o usuário deverá obter autorização e aprovação formal com sua gerência e informar ao departamento de Segurança de Informação quais informações serão copiadas. Ao efetuar a transferência para o dispositivo, fica definido que as informações transportadas passam a ser de responsabilidade do solicitante. Caso a pessoa queira copiar informações do dispositivo para a rede, as informações poderão sofrer inspeção para garantir a segurança e a integridade das informações.

3.13. Admissão e Demissão de Funcionários

O responsável pelo recrutamento e Seleção de funcionários deve informar a área de Segurança de Informação, toda e qualquer movimentação de temporários, estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da Augme. Esse cadastramento inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema. Cabe ao responsável pela contratação a comunicação ao departamento de Segurança da Informação sobre as rotinas que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que ele prestará serviço à Augme, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão, o RH deverá comunicar o fato o mais breve possível ao departamento de Segurança da Informação, para que o funcionário tenha seus acessos físico, à rede e sistemas bloqueados.

Cabe ao RH fornecer conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança. Nenhum funcionário, estagiário ou temporário, poderá ter acessos aos sistemas, sem ter expressamente concordado com esta política.

3.14. Acesso Remoto

A Augme permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, conforme requisição por estes e autorização pelo Diretor de *Compliance/PLDFT*, sendo que os Colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso; (ii) manter softwares de proteção contra malware/antivírus nos dispositivos

remotos; (iii) relatar ao Diretor de *Compliance/PLDFT* qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Augme e que ocorram durante o trabalho remoto; e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

3.15. Controle de Acesso

O acesso pelos Colaboradores nas dependências da Augme é realizado por meio de crachá de acesso ou chave, pessoal e intransferível (biometria), o qual é disponibilizado a cada Colaborador no momento de sua contratação pela Augme.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da Augme, que não poderão ser compartilhados com outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

Tendo em vista que a utilização de computadores, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Augme monitora a utilização de tais meios.

3.16. Firewall, Software, Varreduras e Backup

A Augme utilizará um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Risco será responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede).

A Augme manterá 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). Serão conduzidas varreduras semanalmente para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Augme.

A Augme utilizará um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Risco será responsável por patches regulares nos sistemas da Augme e deverá enviar mensalmente relatório ao Diretor de *Compliance/PLDFT.*

A Augme manterá e testará regularmente medidas de backup consideradas apropriadas pelo Diretor de Risco. As informações da Augme são atualmente objeto de backup diário com o uso de computação na nuvem.

3.17. Monitoramento e Testes

O Diretor de *Compliance/PLDFT* (ou pessoa por ele incumbida) adotará as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, **semestral**:

(i) Deverá monitorar, por amostragem, o acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;

(ii) Deverá monitorar, por amostragem, as ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Augme para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da Augme; e

(iii) Deverá verificar, por amostragem, as informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de *Compliance/PLDFT* poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

3.18. Plano de Identificação e Resposta

- *Identificação de Suspeitas*

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

Ademais, o Diretor de *Compliance/PLDFT* e Diretor de Risco determinarão quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

- *Procedimentos de Resposta*

O Diretor de *Compliance/PLDFT* com auxílio do Diretor de Risco responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Augme 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 Augme, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial); e

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

3.19 Proteção de Dados Pessoais

Escopo e Abrangência:

A Augme está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do seu site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Augme, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Gestora.

É importante observar que o escopo da proteção de dados pessoais no âmbito da Augme está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas. Também estão abrangidos por esta proteção os dados os candidatos às vagas na Gestora, os fornecedores e outros com os quais a Augme manteve contato para atender alguma demanda relevante e específica. Ressalta-se que, são considerados dados pessoais informações que possam identificar um indivíduo como: nome, endereço, telefone, e-mail entre outros.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Augme está pautado nos requisitos do artigo 7º da Lei Geral de Proteção de Dados, assim como nas premissas do artigo 11 da mesma Lei, quando aplicável. Dessa maneira, o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I. quando o titular consentir, de forma específica e clara, para finalidades específicas;

II. sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei Geral de Proteção de Dados e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Princípios Norteadores:

A Augme compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da Lei 13.709/2018:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18, da Lei 13.709/2018, o titular dos dados pessoais tem direito de solicitar à Augme, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o quanto segue abaixo. Todavia o seu exercício em face da Augme deve ser analisado em cada caso concreto.

a) confirmação de existência de tratamento;

b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizado;

d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;

e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;

g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

i) revogação do consentimento, nos termos da Lei.

A Augme disponibiliza canal de comunicação, através do endereço dpo@augme.com, por meio do qual o seu Encarregado pelo Tratamento de Dados Pessoais, o Sr. Fábio Guilhon Chung, receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na Lei Geral de Proteção de Dados em consonância a sua Política de Privacidade. O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer (DPO), é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a Augme, os titulares dos dados (pessoas físicas) e a Autoridade Nacional de Proteção de Dados (ANPD).

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela Augme durante o período de tempo necessário para o atingimento dos objetivos para os quais foram coletados. Porém, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual.

Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Augme estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à Augme, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Augme cooperará com a ANPD em qualquer problema em relação à proteção de dados e dentro dos limites previstos na Lei e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Governança:

As matérias relacionadas aos dados pessoais, dados sigilosos e aos tratamentos destes serão apresentados pelo DPO para deliberação no Comitê de Gestão de Riscos e de Compliance.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao DPO sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Augme para a devida apuração. Caso necessário, o DPO notificará, em prazo compatível com a severidade do evento, a ANPD.

Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos e no Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, nos termos do artigo 38 da Lei Geral de Proteção de Dados.

3.20. Arquivamento de Informações

De acordo com o disposto nesta Política de Segurança da Informação, os Colaboradores 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, em conformidade com a disposição do artigo 34 da Resolução 21 da CVM, pelo prazo de 5 (cinco) anos ou superior, nas hipóteses exigidas pela legislação e regulamentação em vigor.

3.21. Treinamento

O Diretor de *Compliance/PLDFT* organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de *compliance* (conforme descrito no Manual de Conduta e Ética).

4. REVISÃO DA POLÍTICA

O Diretor de Risco deverá realizar uma revisão desta Política de Segurança da Informação a cada vinte e quatro meses, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, devendo submeter a aprovação da nova política à aprovação do Comitê de *Compliance*.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Augme e acontecimentos regulatórios relevantes.

5. ÁREAS VALIDADORAS

- Tecnologia da Informação
- Diretoria de Risco
- Diretor de *Compliance/PLDFT*

ANEXO I - DECLARAÇÃO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

O Colaborador declara ter recebido, lido e aderido à Política de Segurança da Informação e Segurança Cibernética da AUGME CAPITAL GESTÃO DE RECURSOS LTDA.

O Colaborador está ciente de que a violação desta Política o sujeitará não somente às penalidades do Manual de Conduta e Ética, mas também às penalidades da Lei.

Nome: _____

Posição: _____

Assinatura:[1] _____

Data:

[1] Esse documento pode ser assinado digitalmente ou aceito através do sistema de Compliance da Gestora, caso em que será dispensada a via física.