	Nome:	**Política de Segurança da Informação e Segurança Cibernética**	Adotado:	Jan/2019
	Versão:	5ª	Atualizado:	Jan/2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

augme CAPITAL	Nome:	**Política de Segurança da Informação e Segurança Cibernética**	Adotado:	Jan/2019
	Versão:	5ª	Atualizado:	Jan/2026

ÍNDICE

	Nome:	**Política de Segurança da Informação e Segurança Cibernética**	Adotado:	Jan/2019
	Versão:	5ª	Atualizado:	Jan/2026

1. Objetivo

A política de segurança da informação e segurança cibernética ("Política de Segurança da Informação") dispõe sobre a recepção, armazenamento e utilização das informações corporativas e pessoais disponibilizadas aos funcionários 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. 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. Objetivos da Segurança da Informação

(i) Confidencialidade: Garantir que as Informações Confidenciais sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
(ii) Integridade: Garantir que as informações sejam mantidas íntegras, sem modificações indevidas, seja acidental ou proposital;
(iii) Disponibilidade: Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

4. Identificação de Riscos (*Risk Assessment*)

No âmbito de suas atividades, a Augme 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, 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);
(ii) Sistemas: informações sobre os sistemas utilizados pela Augme 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 Augme;
(iv) 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:

(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.

Com base no disposto acima, a Augme avalia e define um conjunto de procedimentos preventivos, que objetivam a mitigação ou mesmo a eliminação do risco do uso indevido de informações, assim como a invasão do ambiente físico e/ou virtual da Augme.

5. Procedimentos Preventivos

5.1 Ações de Prevenção e Proteção

Após a identificação dos riscos, a Augme adota medidas para proteger suas informações confidenciais, a saber:

(i) Uso restrito a Colaboradores, e não devem ser divulgadas a terceiros;
(ii) Controle sobre o ciclo de vida da Informação Confidencial: início até a destruição, quando for o caso;
(iii) Processos e controles sobre os meios físicos e virtuais que contém informações confidenciais;
(iv) Procedimentos para guarda e manutenção de informações e dados;

5.2. 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 e mídias de armazenamento removível, dentre outros, não podem ser utilizadas para guarda ou

transferência de informações confidenciais da Augme, salvo necessidade para realização de suas funções.

A utilização dos ativos e sistemas da Augme — incluindo computadores, telefones, acesso à internet, e-mail corporativo, plataformas aprovadas pelo Compliance para mensagens instantâneas (como o Microsoft Teams) e demais dispositivos — destina-se prioritariamente ao desempenho das atividades profissionais.

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.

É responsabilidade do Colaborador zelar pelos aparelhos e equipamentos disponibilizados, bem como manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

5.3 Uso de senhas

As senhas de acesso devem receber o mesmo nível de proteção atribuído a quaisquer outras credenciais utilizadas rotineiramente. A Augme adota mecanismos de controle destinados a garantir a utilização segura de senhas. Para reforçar essa proteção, aplicam-se as diretrizes abaixo:

I. É vedado divulgar ou compartilhar senhas com terceiros, independentemente da função ou nível de acesso;
II. É desaconselhada a reutilização de senhas antigas ou a utilização da mesma senha em diferentes sistemas
III. É proibido registrar senhas em arquivos digitais ou em anotações físicas suscetíveis de acesso por pessoas não autorizadas;
IV. Deve-se assegurar que o processo de digitação de senhas ocorra sem a possibilidade de observação por terceiros;
V. As senhas devem ser imediatamente alteradas sempre que houver suspeita de comprometimento, devendo o fato ser comunicado à área de Compliance;
VI. Devem ser realizadas alterações periódicas de senhas, conforme políticas internas e requisitos dos sistemas;
VII. As senhas devem seguir critérios mínimos de complexidade, incluindo combinações de letras, números e caracteres especiais;
VIII. Sempre que disponibilizada, a autenticação multifator (MFA) deve ser habilitada para reforçar a segurança das credenciais.

A fim de fortalecer a cultura de gestão de senhas, a Augme disponibiliza aos seus Colaboradores um cofre de senhas corporativo, que permite armazenar credenciais de forma segura, reduzir o risco de vazamentos e facilitar o uso de senhas fortes e exclusivas.

Adicionalmente, o Colaborador poderá ser responsabilizado caso disponibilize a terceiros suas credenciais de acesso individuais — incluindo login e senha — para quaisquer fins, excetuadas as situações formalmente autorizadas pela área competente.

5.4 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 bloquear seu computador com senha.

5.5 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. É solicitado máxima 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.

(i) Não acesse sites ou arquivos, tampouco responda ou envie mensagens eletrônicas de conteúdo que possa afetar a moral pessoal e da organização;
(ii) Não envie mensagens ou acesse sites que afetem a produtividade de sua função;
(iii) Verifique as opções de segurança disponíveis no site visitado;
(iv) 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;
(v) Não leia mensagens de origem desconhecidas, com nome de remetentes ou títulos estranhos. Apague-as imediatamente;
(vi) Não execute programas ou abra arquivos que não são esperados, mesmo que sejam provenientes de origem conhecida ou aparentemente inofensivos;
(vii) Não envie mensagens contendo anexos que não foram incluídos intencionalmente por você; e

(viii) 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.

5.6 Utilização de computação móvel

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

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

5.7 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.

O meio de comunicação formal é sempre via e-mail, sistemas de mensagem instantânea aprovados (Microsoft teams) ou ligação gravada. Qualquer outro canal de comunicação não será tratado um canal formal.

5.8 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.

5.9 Dispositivos Removíveis

Os dispositivos móveis não estão habilitados. Caso necessário à utilização de mídias de armazenamento como *pendrive* e dispositivos similares para transporte de informações da organização, o usuário deverá obter autorização junto a área de Compliance, que somente vigorará até que se tenha efetuado a transferência dos dados solicitados.

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.

5.10 Admissão e Demissão de Funcionários

O responsável pelo recrutamento e seleção de Colaboradores 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 definição e a comunicação ao Suporte de IT sobre os acessos virtuais ao qual o Colaborador terá. No caso de desligamento, o RH deverá comunicar o fato o mais breve possível ao Suporte de IT para que o Colaborador tenha seus acessos físico, à rede e sistemas bloqueados.

5.11 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 da área de Compliance, 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.

5.12 Controle de Acesso

O acesso pelos Colaboradores nas dependências da Augme é realizado por meio de biometria. É terminantemente proibido que o Colaborador facilite ou permita o acesso de pessoas não autorizadas as dependências da Augme.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos na nuvem, 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.

5.13 Firewall, Software, Varreduras e Backup

A Augme utiliza 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.

5.14 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. Tais medidas poderão ser realizadas periodicamente, conforme critérios definidos internamente, ou sempre que houver decisão da administração ou suspeita de comprometimento, violação ou risco relevante.

(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.

5.15 Plano de Identificação e Resposta

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.

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.

5.16 Proteção de Dados Pessoais

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.

Quaisquer dados pessoais de terceiros eventualmente acessados pela Augme em razão da titularidade de títulos de crédito ou instrumentos similares são armazenados em ambiente segregado, com controles de segurança reforçados, isolado dos demais sistemas internos e acessível exclusivamente aos Colaboradores que detenham necessidade estritamente justificada de acesso para a execução de suas funções. O tratamento desses dados segue os mesmos padrões de confidencialidade, integridade e disponibilidade previstos nesta Política, assegurando que o acesso seja sempre proporcional, registrado e limitado ao mínimo necessário.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Augme está pautado nos requisitos Lei Geral de Proteção de Dados. 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;

e) Proteção da vida ou da incolumidade física do titular ou de terceiros;

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 na 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.

<u>Princípios Norteadores:</u>

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.

<u>Direitos:</u>

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).

<u>Período de Armazenamento dos Dados Pessoais:</u>

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.

5.17 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 pelo prazo de 5 (cinco) anos ou superior, nas hipóteses exigidas pela legislação e regulamentação em vigor.

5.18 Treinamento

A área de Compliance 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, descrito no Código de Ética e Conduta.

6. 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.