Política de Segurança da Informação e Cibernética

Uso Interno

Março 2022

ÍNDICE

1. Introdução

A **AZIMUT BRASIL WEALTH MANAGEMENT ("AZBWM")** que é composta pelas empresas **AZIMUT BRASIL WEALTH MANAGEMENT LTDA ("GESTORA")** e **AZIMUT BRASIL DTVM LTDA ("DTVM")** alinhadas com as diretrizes do Grupo Azimut, estabelece sua Política de Segurança da Informação e Cibernética ("Política").

O tema da Segurança Cibernética está sendo incluído a esta Política de Segurança da Informação em atenção ao disposto na Resolução n° 4.893/21 editada pelo Conselho Monetário Nacional do Banco Central do Brasil ("BACEN") de 26 de fevereiro de 2021, o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, entre outros normativos regulatórios.

Parte integrante do Grupo Azimut, a AZBWM tem a sua composição acionária detida pela AZ Brasile Holding Ltda.

2. Público Alvo

As regras contidas nesta Política aplicam-se às pessoas vinculadas.

Definimos como Pessoas Vinculadas:

- Todos os Sócios, profissionais com vínculo CLT e estagiários;
- Administradores, colaboradores, empregados, menores aprendizes, estagiários, correspondentes, prestadores de serviços a terceiros e todas e/ou quaisquer pessoas e demais prepostos que tenham acesso aos dados da AZBWM ou por ela controlados e aos sistemas por ela utilizados e/ou com qualquer sociedade pertencente ao grupo econômico da AZ Brasile Holding que desempenhem atividades na AZBWM e AZ Brasile Holding Ltda;
- São ainda consideradas Pessoas Vinculdas os Agentes Autônomos de Investimentos (AAI) que prestem serviços ao intermediário;
- Profissionais que mantenham contrato de prestação de serviços com a AZBWM e AZ Brasile Holding Ltda;
- Pessoas naturais que sejam, direta ou indiretamente, controladoras ou participem do quadro societário da AZBWM ou AZ Brasile Holding Ltda;
- Sociedades controladas, direta ou indiretamente, pela AZBWM, ou por pessoas a elas vinculadas.

As Pessoas Vinculadas têm os seguintes direitos e responsabilidades:

- Zelar por todo acesso ao ambiente computadorizado executado e registrado com a sua identificação de acesso;
- Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
- Utilizar os recursos tecnológicos (equipamentos, programas e sistemas) e as informações somente para desempenho das suas atividades profissionais, sendo assim vedado o seu uso para fins pessoais;
- Não discutir, citar ou compartilhar assuntos confidenciais em ambientes públicos ou em áreas expostas (aviões, transportes, restaurantes, encontros sociais etc.), incluindo comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo; e

- Comunicar imediatamente à Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas normas e procedimentos.

O descumprimento de quaisquer das diretrizes estabelecidas por esta Política será considerado infração grave, sujeitando seu autor às sanções cabíveis, nos termos da legislação aplicável.

3. Objetivo

A Política de Segurança da Informação e Cibernética da AZBWM tem o objetivo de assegurar a confidencialidade, integridade e a disponibilidade dos dados e dos sistemas de informação, dos veículos de investimentos sob sua gestão, dos seus clientes, investidores e/ou Pessoas Vinculadas, além de estabelecer suas regras, procedimentos e controles de segurança para tratar destes objetivos, uso e funcionamento da sua infraestrutura de tecnologia.

A presente Política aplica-se a todos os processos, operações, sistemas, informações da AZBWM, de forma a prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético da AZBWM.

4. Princípios de Segurança da Informação e Cibernética

Para os fins desta Política, informações confidenciais são as informações e/ou todo e qualquer conteúdo ou dado que tenha valor para a AZBWM, veículos de investimentos sob sua gestão, seus clientes, investidores e/ou Pessoas Vinculadas, ou, ainda, informações que ainda não sejam de domínio público ou que a AZBWM não deseje que sejam divulgadas. Dessa forma, é terminantemente proibida a divulgação de informações confidenciais para fora dos escritórios da AZBWM ou para pessoas, mesmo que dentro ou fora da AZBWM, que não necessitem ou não devam ter acesso a tais informações.

A proteção e privacidade de dados dos clientes refletem os valores da AZBWM e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

A Segurança da Informação e Cibernética é aqui caracterizada pela preservação da:

- **Confidencialidade**, que é a garantia de que a informação tratada pela AZBWM é acessível somente a pessoas com acesso autorizado, impedindo a exposição de dados restritos e acessos não autorizados;
- **Integridade**, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento, de forma que elas sejam íntegras e sem alterações feitas por pessoas não autorizadas;
- **Disponibilidade**, que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.
- **Acesso Controlado**, que é o acesso restrito e controlado dos usuários à uma determinada informação, através de mecanismos de controle de acesso, de acordo com o nível e sigilo e acesso

Qualquer informação sobre a AZBWM, suas atividades, seus sócios e clientes só poderá ser fornecida ao público, mídia ou a demais órgãos mediante autorização prévia da área do Compliance

5. Diretrizes de Segurança da Informação e Cibernética

O cumprimento desta Política é de responsabilidade de todas as Pessoas Vinculadas as quais devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
- Somente deve ser concedido acesso às informações e recursos de informação imprescindíveis para o pleno desempenho das atividades da Pessoa Vinculada autorizada;
- As informações da AZBWM, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;
- Todo processo, durante seu ciclo de vida, deve garantir a segregação de funções;
- Assegurar que as informações e os dados devem ser utilizados de forma transparente e apenas para as finalidades para as quais foram coletadas;
- A identificação de qualquer pessoa vinculada deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo pessoal e intransferível proibido e vedado seu compartilhamento; Os riscos às informações, eventuais fatos ou ocorrências que possam colocar em risco tais informações, da AZBWM devem ser reportados à área de Tecnologia da Informação será responsável pelo registro e controle dos efeitos de incidentes relevantes; e
- As responsabilidades quanto à Segurança da Informação e Cibernética devem ser amplamente divulgadas às Pessoas Vinculadas, que devem entender e assegurar o cumprimento desta Política e seu Procedimento de Segurança da Informação.

No tratamento da Informação e classificação de dados e informações devem ser considerados:

- A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética e da Informação da AZBWM em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.
- As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Não classificada (Pública), Uso Interno, Restrita e Confidencial. Este assunto também está disponível no Código de Ética e Conduta em "Controle da Informação e Confidencialidade" e no Procedimento de Segurança da Informação.

6. Responsabilidades

É de responsabilidade de cada Diretorias ou Gerências levar em consideração os cenários de ameaças previstos na avaliação de risco.

6.1. Diretorias e Gerências

- Deverão acompanhar e apoiar as áreas sob sua responsabilidade, certificando-se de que as mesmas estejam em conformidade com a regulamentação e normas aplicáveis aos negócios da instituição e comprometendo-se com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; bem como respeitar e fazer com que suas equipes cumpram as políticas, manuais e procedimentos internos estabelecidos e implementados na AZBWM.

6.2 Área deTecnologia da Informação (TI)

- Manter atualizado esta Política e outros Normativos Corporativos relacionados à área;
- Monitorar o cumprimento das regras estabelecidas;
- Estabelecer diretrizes que possam responder às mudanças dos negócios, da legislação, das normas regulatórias e da tecnologia;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Estabelecer as regras de proteção dos bens da informação, quanto aos acessos, backups, entre outros;
- Responder pelas violações registradas e participar da decisão a ser tomada, quando da ocorrência de não conformidade;
- Controlar e resolver as não-conformidades de segurança;
- Administrar e controlar o acesso físico e lógico à informação respeitando a segregação de área e função;
- Simular, executar e regitrar os Planos de Continuidade; e
- Promover ações de conscientização sobre segurança da informação e cibernética às pessoas vinculadas;

6.3 Compliance

- Informar mudanças regulatórias que, de alguma forma, possam impactar esta Política;
- Reportar à Diretoria situações de descumprimento das regras desta Política;
- Acompanhar constantemente os riscos cibernéticos, baseados nas orientações de segurança fornecidas pela Área de Tecnologia da Informação da AZBWM.

6.4 Auditoria Interna

- Revisar e avaliar a eficiência quanto à implementação e aos controles da instituição.

6.5 Jurídico

- Assegurar que contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da AZBWM contenham cláusulas que assegurem o cumprimento desta Política e das Normas de Segurança da Informação e Cibernética, bem como penalidades no caso de descumprimento.

7. Riscos Cibernéticos

Com o aumento exponencial das ameaças cibernéticas, a AZBWM criou uma estrutura para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes. À luz da Lei Geral de Proteção de Dados Pessoais[1], deve-se considerar que a segurança cibernética é um dos componentes para que a privacidade do titular seja assegurada por mecanismos de proteção de dados. Em relação aos riscos relacionados à segurança cibernética, a AZBWM verificou, nos termos do Guia ANBIMA de Cibersegurança[2], os principais motivos e ameaças para os seus negócios:

- Revelação de informações sensíveis e obter vantagens competitivas com esses dados;
- Modificações indevidas de dados e programas;
- Perda de dados e programas;
- Destruição ou perda de recursos computacionais e instalações;
- Interdições ou interrupções de serviços essenciais.

São riscos de ataques cibernéticos, ainda, oriundos de malware[3], técnicas de engenharia social[4] invasões e ataques de rede (DDoS e Botnets)[5], fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

As ameaças cibernéticas podem variar de acordo com a natureza, a vulnerabilidade e as informações ou os bens de cada empresa. As consequências para a AZBWM podem ser significativas em termos de risco de imagem, danos

1 Lei nº 13.709, de 14 de agosto de 2018.

2 Esta 3ª edição do Guia foi publicada em junho de 2021 (1ª edição publicada em 3/8/16).

3 *Softwares* desenvolvidos para corromper a segurança da rede de computadores como vírus, *ransomware, spyware, phishing* etc.

4 Método que manipula o conhecimento dos usuários da instituição para obter principalmente informações confidenciais da empresa.

5 Ataques cibernéticos, normalmente realizados por *hackers*, que utilizam meios para explorar fragilidades e deficiências específicas do ambiente tecnológico, podendo causar a interrupção temporária e/ou a continuidade dos seus negócios.

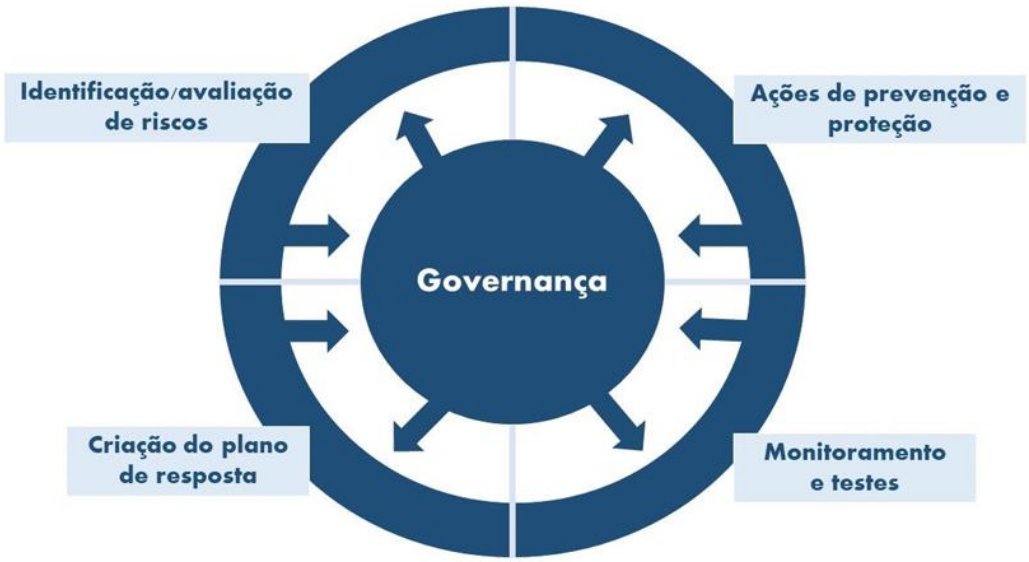
financeiros ou perda de vantagem concorrencial, além de riscos operacionais. Os possíveis impactos dependem ainda da rápida detecção e resposta após a identificação do ataque pela área de Tecnologia da Informação da AZBWM.

A lista demonstrada acima não pretende ser exaustiva e serve para exemplificar os principais fatores de risco que a AZBWM pode estar exposta no curso normal das suas atividades. Estes riscos serão constantemente acompanhados pelas equipes de Risco e Compliance, baseados nas orientações de segurança fornecidas pela área de Tecnologia da Informação da AZBWM.

8. Processo de Segurança da Informação e Cibernética

Para que a AZBWM, em consonância com o Guia de Cibersegurança da ANBIMA, tenha um programa eficiente contra ameaças cibernéticas, ela deve, no mínimo, desempenhar cinco funções:

[6]



Para assegurar que as informações tratadas estejam adequadamente protegidas, segue o detalhamento das cinco funções como são adotadas na AZBWM:

[6] Imagem extraída da 3ª edição do Guia de Cibersegurança da ANBIMA publicado em junho de 2021.

a) Identificação/avaliação de riscos (risk assessment): A AZBWM utiliza programas e controles de segurança cibernética que atendem suas necessidades, elaborando e mantendo uma avaliação de riscos atualizada. A partir do momento que um risco é identificado, são realizadas as análises/avaliações qualitativas quantitativas, buscando avaliar o contexto em que o risco está enquadrado. Uma vez definidos os riscos, ações de prevenção e proteção devem ser tomadas.

b) Ações de prevenção e proteção: A AZBWM utiliza algumas ferramentas para manter a segurança dos sistemas e dados. A regra básica é restringir e monitorar o acesso físico e virtual às informações críticas/sensíveis.

Os ativos da informação[7] devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente (configurações de blindagem ou "*hardening", patch management*, autenticação e autorização) e ter documentação e planos de manutenção atualizados periodicamente.

As instalações, equipamentos, redes e sistemas de computadores, possuem mecanismos de controle de acesso físico e/ou lógico, que possibilitam a identificação das pessoas.

O controle é feito por meio dos perfis de acesso, que segregam as funções realizadas pelas diversas áreas da AZBWM. Cada área possui um conjunto de perfis relacionados às suas atividades, e a AZBWM dispõe de procedimentos para que o acesso seja liberado mediante aprovação.

Os acessos às informações e aos ambientes tecnológicos são controlados de acordo com sua classificação e revisados periodicamente, de forma a serem disponibilizados apenas às pessoas autorizadas e com os privilégios necessários para o desempenho de suas atividades.

Os acessos são rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente a pessoa vinculada, para que seja responsabilizado por suas ações. As senhas devem ser definidas sempre com alta complexidade, e quando possível, com autenticação de múltiplos fatores. A AZBWM proíbe o reaproveitamento de senhas e recomenda o uso de um gerenciador de senhas ao invés da repetição da mesma senha, por mais sofisticada que seja, para facilitar a memorização em vários serviços.

Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura da AZBWM. É desabilitado aos seus usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de infraestrutura. Os eventos de login e alteração de senhas são auditáveis e rastreáveis, assim como os acessos a equipamentos, softwares e respectivas permissões são testados periodicamente pela área de Infraestrutura de Tecnologia.

[7] Entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação.

A AZBWM implementou o Web Filtering (Filtro de Conteúdo Web) através da instalação de Firewall na sua rede corporativa, com objetivo garantir esforços contínuos para proteção dos ativos de informação.

A AZBWM conta com recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais. Da mesma maneira monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas. A

AZBWM realiza, também, backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Continuidade do Negócio.

c) Monitoramento e testes: A AZBWM possui mecanismos e sistemas de monitoramento para cada um dos controles existentes, implementados de acordo com uma abordagem baseada em risco e intensificados de acordo com o nível de ressico, sempre considerando o contexto no qual a AZBWM está inserida e suas necessidades emergentes. A AZBWM realiza, periodicamente, testes de invasão externa e phishing, plano de resposta a incidentes bem como, análises de vulnerabilidades na sua estrutura tecnológica.

d) Criação de plano de resposta: O plano de resposta é vital para proteger as atividades da AZBWM e foi elaborado com o envolvimento de múltiplas áreas, incluindo a Diretoria. Os recursos tecnológicos disponibilizados pela AZBWM serão monitorados por software que fornecerá, de forma automática, informações atualizadas sobre as tentativas de invasão e a possível indisponibilidade de algum serviço. Por meio da análise das informações fornecidas em relatórios, a AZBWM poderá verificar a necessidade ou não da tomada de alguma providência. Os Colaboradores que identificarem situações de risco iminente, deverão informar imediatamente a área de Tecnologia da Informação para que inicie os procedimentos de avaliação de um suposto ataque cibernético. A área de Tecnologia da Informação comunicará imediatamente, para as Diretorias e Gerências os incidentes que possam gerar riscos à AZBWM, levando em consideração os cenários de ameaças previstos na avaliação de risco.

e) Governança: A AZBWM tem o Comitê de Segurança da Informação e Cibernética que é o fórum para tratar da sua segurança cibernética, com representação e governança apropriadas. O Comitê reunirá as informações relevantes, sobre segurança da informação e cibernética ocorridas e apresentará, juntamente com o Comitê de Risco e Compliance, aos Diretores da AZBWM.

Na hipótese de violação de dado pessoal, o Encarregado de Dados e o Comitê de Segurança da Informação e Cibernética deverão conjuntamente avaliar o seu impacto para os titulares e, se for o caso, informá-los, bem como à Autoridade Nacional de Proteção de Dados – ANPD.

Ademais, o programa de segurança cibernética é revisado periodicamente mantendo sempre atualizadas suas avaliações de risco, implementações de proteção, planos de resposta a incidentes e monitoramento dos ambientes, conforme exposto abaixo.

Acesso Remoto (VPN)

Utilizamos uma Rede Virtual Privada (VPN) que permite que os profissionais autorizados se conectem com segurança a rede privada da empresa, garantindo continuidade dos negócios da instituição. Assim, o usuário navega através de uma conexão encriptada, mitigando risco com privacidade e uso de dados.

O acesso à VPN de cada profissional é criado e controlado pela equipe de TI. A autenticação personalizada garante que apenas os usuários ativos e autorizados possam acessar a rede corporativa, mediante uso de login e senha. Os antivírus e Firewalls também contribuem para um ambiente mais seguro.

As senhas são renovadas periodicamente e possuem regras para criação de senhas seguras.

Cada profissional acessa apenas sistemas e diretórios de rede pertinentes a sua atividade e de acordo com a segregação de acessos. Os sistemas requerem o uso de senha do usuário, aumentando a segurança da informação. A equipe de TI monitora e dá suporte aos usuários.

O procedimento e regras de Acesso Remoto VPN está descrito em documento específico.

9. Fornecedores e partes externas

Os contratos da AZBWM com as empresas prestadoras de serviços deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, bem como cláusulas que garantam que os profissionais das empresas prestadoras de serviços: (i) protejam e zelem pelo sigilo das informações da AZBWM e (ii) tenham conhecimento, concordância e cumprimento desta Política.

Adicionalmente, as empresas prestadoras de serviços devem cumprir as leis e normas que regulamentam a propriedade intelectual e a proteção de dados, especialmente a Lei Geral de Proteção de Dados Pessoais e a Resolução nº 4.893/2021 do Banco Central do Brasil, e utilizar os dados da AZBWM, ou por ela controlados, os sistemas por ela utilizados, bem como os ambientes físico e tecnológico da Instituição, apenas para as finalidades objeto do contrato de prestação de serviço.

Por fim, AZBWM somente contratará prestadores de serviços que demonstrarem a adoção de mecanismos de prevenção e tratamento de incidentes, tais como: (i) software de proteção contra softwares maliciosos, mantendo-o sempre ativado e atualizado; (ii) Firewall, mantendo-o sempre ativado e atualizado; (iii) mecanismos de controles de acesso e de autenticação que permitam identificar e rastrear o usuário que tiver acesso aos sistemas ou dados da AZBWM e seus clientes no ambiente cibernético; (iv) mecanismos de criptografia que permitam criptografar os dados pessoais de clientes e os dados pertencentes à AZBWM armazenados pelo prestador de serviço ou enviado por meios de comunicação; e (v) mecanismos de segmentação da rede pela qual o prestador de serviço acessa aos sistemas ou dados da AZBWM ou seus clientes; (v) planos de resposta a incidentes de Cibersegurança, canais de gestão apropriados para receber o relato da detecção de incidentes, o mais rápido possível, além de política de comunicação a clientes e/ou reguladores na hipótese de ocorrência desses incidentes.

10. Descarte de informações

O descarte da informação deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital. A informação deve ser descartada considerando prazos

mínimos legais, regulatórios, e contratuais aplicáveis, bem como sua necessidade para o negócio ou a área, o que for maior. O Comitê de Segurança da Informação e Cibernética é responsável pela implantação de cronograma para o descarte periódico de dados pessoais, bem como monitoramento do processo de eliminação e definição do método mais adequado.

11. Treinamento

Além do processo de treinamento inicial, a AZBWM oferece treinamentos (online ou presencial) aos quais as pessoas vinculadas são submetidas, com o objetivo de manter uma reciclagem continuada e conscientizá-los sobre confidencialidade das informações, segurança da informação e cibernética, proteção de dados pessoais entre outras potenciais ameaças à integridade dos sistemas de informação.

Consideramos que os Comunicados enviados pela TI, são também uma forma de treinamento, orientação e reforço dos temas relacionados à Segurança da Informação, Segurança Cibernética e Proteção de Dados.

A TI também poderá utilizar a Intranet, disponível para os colaboradores, guias de conscientização sobre essas ameaças e de como se proteger delas e responder a elas.

12. Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da AZBWM em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

13.Termo de Responsabilidade

No início de suas atividades, a pessoa vinculada contratada participará de um processo de integração e treinamento em que adquirirá conhecimento sobre as atividades da AZBWM, suas normas internas, bem como esta Política, o Código de Ética e Conduta e demais Normativos Corporativos adotados pela AZBWM.

Ao assinar o “Termo de Responsabilidade e Ciência dos Normativos Corporativos” a pessoa vinculada se compromete com a Política de Segurança da Informação e Cibernética da AZBWM e demais Normativos Corporativos da AZBWM.