Política de Segurança da Informação e Cibernética

Uso Interno

Agosto 2020

AZIMUT BRASIL
WEALTH MANAGEMENT

Conteúdo

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.
O tema da Segurança Cibernética está sendo incluída a esta Política de Segurança da Informação em atenção ao disposto na Resolução n° 4658/18 do Banco Central do Brasil ("BACEN") de 26 de abril de 2018, 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 Brasil Holdings Ltda.

2. Público Alvo

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

Definimos como Pessoas Vinculadas:

- profissionais com vínculo CLT e estagiários;
- administradores, empregados e demais prepostos que desempenhem atividades na AZBWM ou em qualquer empresa pertencente ao grupo econômico da AZ Brasil Holdings Ltda;
- Agentes Autônomos de Investimentos (AAI) que prestem serviços ao intermediário;
- profissionais que mantenham contrato de prestação de serviços com a AZBWM ou com qualquer empresa pertencente ao grupo econômico da AZ Brasil Holdings Ltda e AZ Brasil Holdings Ltda;
- pessoas naturais que sejam, direta ou indiretamente, participantes do quadro societário da AZBWM ou de qualquer empresa pertencente ao grupo econômico da AZ Brasil Holdings Ltda;

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 tem por objetivo estabelecer as regras, procedimentos e controles de segurança adotadas pela AZBWM para tratar dos requisitos de privacidade, integridade e disponibilidade das suas informações, seu uso e funcionamento da sua infraestrutura de tecnologia.

A informação é um ativo que, como qualquer outro ativo importante para os negócios, têm um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida. A Segurança da Informação e Cibernética objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

4. Responsabilidades

4.1 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; bem como respeitar as políticas, manuais e procedimentos internos estabelecidos e implementados na AZBWM.
- Acompanhar sua equipe e promover orientação no cumprimento desta política.

4.2 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;
- Promover ações de conscientização sobre segurança da informação e cibernética às pessoas vinculadas;

4.3 Compliance

- Informar mudanças regulatórias que, de alguma forma, possam impactar esta Política.
- Reportar à Diretoria situações de descumprimento das regras desta Política.

4.4 Auditoria Interna

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

4.5 Jurídico

- Assegurar que contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da Companhia contenham cláusulas que assegurem o cumprimento desta Política

e das Normas de Segurança da Informação e Cibernética, bem como penalidades no caso de descumprimento.

4.6 Pessoas Vinculadas

- 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, transporte, restaurantes, encontros sociais etc.), incluindo comentários e opiniões em blogs e redes sociais.
- Não compartilhar informações confidenciais de qualquer tipo.
- Comunicar imediatamente à Segurança da Informação (TI) qualquer descumprimento ou violação desta política e/ou de suas normas e procedimentos.

5. Princípios de Segurança da Informação e Cibernética

A proteção e privacidade de dados dos clientes refletem os valores da AZBWM e reafirmam o seu compromisso com a melhoria continua 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 é acessível somente a pessoas com acesso autorizado;
- **Integridade**, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- **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.

A Segurança da Informação e Cibernética é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, instruções de trabalho e funções de software. Estes controles garantem que os objetivos de segurança específicos da AZBWM sejam atendidos.

Os riscos típicos que pretendemos eliminar ou reduzir são:

- Revelação de informações sensíveis;
- 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;
- Roubo de propriedades.

6. Confidencialidade

As pessoas vinculadas à AZBWM deverão observar as regras de confidencialidade previstas no Código de Ética e Conduta, principalmente no que se refere os tópicos "Controle da Informação e Confidencialidade", "Proteção da Informação"e "Dos Recursos de trabalho oferecidos".

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.

7. Diretrizes

O cumprimento da Política de Segurança da Informação e Segurança Cibernética é de responsabilidade de todas as pessoas vinculadas à AZBWM, os 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;
- 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 os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela AZBWM;
- A identificação de qualquer pessoa vinculada deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- A senha é pessoal e intransferível, sendo proibido seu compartilhamento;
- Os riscos às informações da AZBWM devem ser reportados à área de TI responsável pela Segurança da Informação;
- As responsabilidades quanto à Segurança da Informação e Cibernética devem ser amplamente divulgadas às pessoas vinculadas, que devem entender e assegurar estas diretrizes.

8. Riscos Cibernéticos

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

Relacionamos alguns ataques mais comuns de criminosos cibernéticos.

- **Malwares**

É um programa com código malicioso/mal-intencionado.

Vírus: software que causa danos a máquina, rede, softwares e banco de dados;

Cavalo de Troia: é um *malware* que fica oculto em um arquivo aparentemente normal, e pode executar inúmeras tarefas, entre elas criar uma porta (no computador) para uma possível invasão.

Spyware: *software* malicioso para coletar e monitorar o uso de informações;

Ransomware: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- **Engenharia Social**

Pharming**:** direciona o usuário para um site fraudulento, sem o seu conhecimento;

Phishing**:** links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

Vishing**:** simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

Smishing**:** simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- **Fraudes Externas e invasões**

Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

- **Ataques DDoS e Botnets**

DDoS**:** é um ataque distribuído de negação de serviço, em uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Gerando um grande e repentino número de requisições de acesso a um sistema/servidor, fazendo com que este não seja capaz de atender a mais nenhum pedido.

Dependendo do recurso atacado, o servidor pode chegar a reiniciar ou até mesmo ficar travado.

Botnets**:** é formada pelos termos *robot* e *network* que designa um grupo de computadores conectados à Internet, cada um deles rodando um ou mais *bots* e se comunicando com outros dispositivos, a fim de executar determinada tarefa. O termo é geralmente associado ao uso de software malicioso, e, por isso, carrega uma conotação negativa. *Botnets* têm sido empregados para envio de *spam, adwares, spywares*, vírus, *worms* ou qualquer tipo de ataque digital (como um ataque DDoS).

9. Processo de Segurança da Informação e Cibernética

Para assegurar que as informações tratadas estejam adequadamente protegidas, a AZBWM adota os seguintes processos:

9.1 Gestão de Ativos

Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação.

- **Ativos de informação:** base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
- **Ativos de *software*:** aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- **Ativos físicos:** equipamentos computacionais (*hardware*), equipamentos de comunicação, mídias removíveis e outros equipamentos;
- **Serviços:** serviços de computação e comunicações, utilidades gerais, como aquecimento, iluminação, eletricidade e refrigeração;
- Pessoas e suas qualificações, habilidades e experiências;
- Intangíveis, tais como a reputação e a imagem da organização

Os ativos da informação 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 anualmente.

9.2 Gestão de Acessos

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.

9.3 Gestão de Mudanças

A área de Infraestrutura de TI é responsável por participar, documentar, homologar e implementar toda e qualquer alteração seja de acesso, hardware e software ou que tenha impacto direto na infraestrutura de negócio ou operacional da AZBWM.

As solicitações devem ser encaminhadas do gestor responsável pela solicitação para área de infraestrutura de TI, e tais demandas devem ser registradas em sistema para acompanhamento histórico.

9.4 Gestão de Riscos (Risk Assessment)

Os riscos monitorados e identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da AZBWM, para que sejam recomendadas as proteções adequadas. Os cenários de riscos de segurança da informação e cibernéticos são escalonados para a Alta Administração.

9.5 Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

9.6 Classificação da Informação

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".

9.7 Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

9.8 Ações de Prevenção e Proteção

A AZBWM tem implementado o Web Filtering (Filtro de Conteúdo Web) através da instalação de *Firewall* na rede corporativa, com objetivo garantir esforços contínuos para proteção dos ativos de informação. Foi selecionado pelo Compliance em conjunto com a equipe de TI e aprovada pela Diretoria.

A AZBWM conta com recursos anti-malware em estações e servidores de rede, como antivirus 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.

9.9 Programas utilizados no computador

Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura.

É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de infraestrutura.

Os acessos a equipamentos, softwares e respectivas permissões são testados periodicamente pela área de Infraestrutura de Tecnologia.

9.10 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.

9.11 Fornecedores e partes externas

Os contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da Companhia devem conter cláusulas que assegurem o cumprimento das regras de segurança da informação, bem como penalidades no caso de descumprimento.

9.12 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 ou regulatórios, bem como sua necessidade para o negócio ou a área, o que for maior.

9.13 Plano de Ação e resposta a Incidentes

Os colaboradores e prestadores de serviço tem como obrigação e responsabilidade conforme ítens anteriores, de reportar diretamente a área de TI todo e qualquer suspeita, bem como incidências atípicas relacionadas ao tema.

Além disso a área de TI e infraestutura realizam a avaliação destas ocorrências. Aquelas avaliadas pela equipe de TI como baixo grau de impacto são tratadas pela equipe de TI. As ocorrências de médio e/ou alto grau de impacto, devem ser reportadas pelo TI aos membros da diretoria para a apresentação, discussão, análise de seus impactos e devida correção.

Periodicamente (mensalmente) a equipe de TI e provedor de infraestrutura elaboram relatório com um resumo da utilização e consumo de toda a infraestrutura bem como eventuais incidentes que tenha ocorrido.

9.14 Treinamento

Além do processo de treinamento inicial, a AZBWM oferece treinamentos aos quais as pessoas vinculadas são submetidos, com o objetivo de manter uma reciclagem continuada e conscientizá-los sobre confidencialidade das informações, segurança da informação e cibernética, 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 a Segurança da Informação e Segurança Cibernética.

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.

9.15 Testes periódicos

A AZBWM realiza testes periódicos de segurança para os sistemas de informações (sem se limitar a, mas em especial, para os meios eletrônicos) anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

10. 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.

11. Termo de Responsabilidade

No início de suas atividades, a pessoa vinculada contratada participará de um processo de integração e treinamento onde 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 vinculdada se compromete com a Política de Segurança da Informação e Cibernética da AZBWM e demais Normativos Corporativos da AZBWM.

12. Divulgação e Transparência

Sempre que necessário são enviados através de e-mail da Tecnologia da Informação comunicados gerais às pessoas vinculadas e/ou comunicados específicos à determinados grupos da instituição para notificação de informação relevante.

As pessoas vinculadas tem acesso ao diretório de rede denominado Intranet, onde ficam publicadas todas os Normativos Corporativos da instituição.

13. Disposições Gerais

Este material foi elaborado pela **AZIMUT BRASIL WEALTH MANAGEMENT ("AZBWM")** que é composta pelas empresas **AZIMUT BRASIL WEALTH MANAGEMENT LTDA ("GESTORA")** e **AZIMUT BRASIL DTVM LTDA ("DTVM")** e não pode ser alterado, copiado, impresso, reproduzido ou distribuído sem prévia e expressa concordância destas.

Todas as pessoas vinculadas devem sentir-se envolvidas e responsáveis pelo aprimoramento dos Controles Internos de forma a mitigar riscos e na busca constante da eficiência e integridade no desempenho das atividades.

O seu descumprimento é passível de aplicação de medidas disciplinares, conforme previsto no Código de Ética e Conduta.