Política de Segurança da Informação e Cibernética

Abril 2024

azimut
wealth management

Conteúdo

1. Introdução

A Azimut Brasil Wealth Management LTDA (“AZBWM”), Azimut Brasil DTVM LTDA (“DTVM”), AZFLOW Consultoria LTDA (“AZFLOW”) e Azimut Brasil Consultoria e Correspondente Bancário LTDA (“CONSULTORIA”) alinhadas com as diretrizes do Grupo Azimut, estabeleceram sua Política de Segurança da Informação e Cibernética.

2. Público Alvo

As regras contidas neste Código aplicam-se às pessoas vinculadas.

Definimos como Pessoas Vinculadas:

- Profissionais com vínculo CLT e estagiários;
- Administradores, empregados e demais prepostos que desempenhem atividades na DTVM ou em qualquer empresa pertencente ao grupo econômico da AZ Brasile Holding Ltda;
- Consultores de Valores Mobiliarios autorizados pela CVM e vinculados às empresas de consultoria do Grupo;
- Assessores de Investimentos (AI) que prestem serviços ao intermediário;
- Profissionais que mantenham contrato de prestação de serviços com a DTVM ou com qualquer empresa pertencente ao grupo econômico da AZ Brasile Holding Ltda;
- Pessoas naturais que sejam, direta ou indiretamente, participantes do quadro societário da DTVM ou de qualquer empresa pertencente ao grupo econômico da AZ Brasile Holding Ltda;

3. Objetivo

A Política de Segurança da Informação e Cibernética visa estabelecer as diretrizes da Azimut Brasil para garantir a confidencialidade, integridade e disponibilidade dos dados e informações sob sua gestão, além de estabelecer suas regras, procedimentos de controles de segurança para tratar destes objetivos, uso e funcionamento da sua infraestrutura de tecnologia.

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 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.

4.2 Área de Tecnologia da informação (TI)

- Manter esta Política e outros Normativos Corporativos relacionados à área atualizados;
- 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;
- Instituir 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 registrar os Planos de Continuidade do Negócio; e
- 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;
- Acompanhar constantemente os riscos cibernéticos, baseados nas orientações de segurança fornecidas pela Área de Tecnologia da Informação.

4.4 Auditoria Interna

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

4.5 Área de Risco

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

5. Princípios da 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 Azimut, 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 companhia não deseje que sejam divulgadas. Dessa forma, é terminantemente proibida a divulgação de informações confidenciais para fora do escritório ou para pessoas, de dentro ou fora da Azimut, que não necessitem ou não devam ter acesso a tais informações.

A proteção e privacidade de dados dos clientes refletem os valores do grupo Azimut 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**: é a garantia de que a informação tratada é acessível somente a pessoas com acesso autorizado, impedindo a exposição de dados restritos e acessos não autorizados;
- **Integridade**: 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**: é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;
- **Acesso Controlado**: é o acesso restrito e controlado dos usuários a uma determinada informação, por meio de mecanismos de controle de acesso, conforme o nível e sigilo e acesso.

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

6. 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 companhia, dos clientes e do público em geral devem ser tratadas de forma ética, sigilosa e conforme 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, intransferível, proibido e vedado seu compartilhamento; os riscos às informações, eventuais fatos ou ocorrências que possam colocar em risco tais informações, da Azimut 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 na classificação de dados e informações, devem ser considerados:

i. A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética e da Informação da Azimut Brasil em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte.

ii. As informações devem ser classificadas segundo 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.

7. Riscos Cibernéticos

Com o aumento exponencial das ameaças cibernéticas, a Azimut 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 Azimut 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 conforme a natureza, a vulnerabilidade e as informações ou os bens de cada empresa. As consequências para a Azimut podem ser significativas em termos de risco de imagem, danos 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.

A lista demonstrada acima não é exaustiva e possibilita exemplificar os principais fatores de risco que a empresa 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 Azimut.

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

[2] A 3ª edição do Guia foi publicada em junho de 2021.

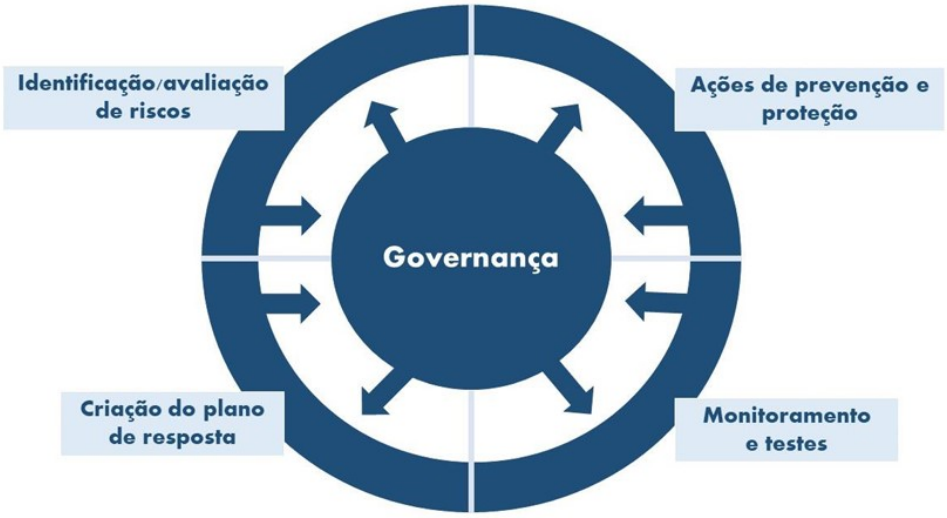
3 Softwares desenvolvidos para corromper a segurança da rede de computadores como vírus, ransomware, spyware, phishing etc.

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.

8. Processo de Segurança da Informação e Cibernética

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



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

a) Identificação/avaliação de riscos (risk assessment): A Azimut 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 e 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 Azimut 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 Azimut. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Azimut dispõe de procedimentos para aprovação dos acessos.

Os acessos às informações e aos ambientes tecnológicos são controlados de acordo com sua classificação e revisados periodicamente, para 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. As senhas devem ser definidas sempre com alta complexidade e, quando possível, com autenticação de múltiplos fatores. É proibido 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. 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.

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

Há também 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.

É realizado 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 Azimut possui mecanismos e sistemas de monitoramento para cada um dos controles existentes, implementados de acordo com uma abordagem baseada em risco e intensificados conforme o nível de risco, sempre considerando o contexto no qual a companhia está inserida e suas necessidades emergentes. A Azimut realiza, periodicamente, o teste de continuidade de negócio, realizando análise de possíveis vulnerabilidades na sua estrutura tecnológica.

d) Criação de plano de resposta: O plano de resposta é vital para proteger as atividades da Azimut e foi elaborado com o envolvimento de múltiplas áreas, incluindo a Diretoria. Os recursos tecnológicos disponibilizados 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 Azimut 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 iniciar 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 companhia, considerando os cenários de ameaças previstos na avaliação de risco.

e) Governança: A Azimut poderá levar ao Comitê de Risco e Compliance quaisquer pontos para tratar a respeito da sua segurança cibernética, com representação e governança apropriadas.

Na hipótese de violação de dado pessoal, o Encarregado de Dados (DPO) deverá reportar ao Comitê de Riscos e Compliance para avaliar o impacto para os titulares e, se for o caso, informá-los, bem como à Autoridade Nacional de Proteção de Dados – ANPD.

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

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

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 acessem 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 conforme 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 as regras de Acesso Remoto VPN estão descritos em documento específico.

9. Fornecedores e partes externas

Os contratos firmados 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 Azimut 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 Azimut, 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, Azimut 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 Azimut e seus clientes no ambiente cibernético; (iv) mecanismos de criptografia que permitam criptografar os dados pessoais de clientes e os dados pertencentes à Azimut 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 companhia 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. Treinamento

Além do processo de treinamento inicial, a Azimut promove treinamento de segurança da informação e cibernética anualmente a todos os vinculados, mantendo assim reciclagem contínua e conscientizando os vinculados a respeito da

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, para publicação de guias de conscientização sobre essas ameaças e de como se proteger delas e responder a elas.

11. Considerações

O descarte da informação deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, conforme 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. A Diretoria de TI 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.

Tratamento da informação: A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da Azimut em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte.

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 Azimut, suas normas internas, bem como esta Política, o Código de Ética e Conduta e demais Normativos Corporativos adotados pela companhia.

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 Azimut e demais Normativos Corporativos.

12. Disposições Gerais

Este material foi elaborado pela Azimut Brasil 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.

13. Base Legal

- Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre segurança cibernética;
- Guia de Cibersegurança da ANBIMA de março de 2021.

14. Informações de Controle

Vigência: 1 ano.

Versão: Abril de 2024

Atendimento a necessidades específicas:

( ) Sox
( ) Basiléia
(X) Outros: Políticas internas da Azimut Brasil
( ) Não Aplicável

Versão	Item alterado	Descrição resumida da alteração	Motivo	Data
1	-	-	Elaboração da Política	Fevereiro 2017
2	Todos	Revisão geral do documento, visto que a primeira versão foi criada pela GESTORA e nesta versão a aplicação está sendo ampliada para AZBWM (GESTORA e DTVM). Inclusão do tema Segurança Cibernética.	Revisão da Política	Março 2019
3	9.10	Inclusão do ítem 9.10 Acesso Remoto VPN	Revisão da Polítca	Setembro 2020
4	1, 2, 9.13,	Atualização da normativa, de dados societários e adequação à LGPD	Revisão da Polítca	Março 2022
5	Todos	Revisão periódica prevista.	Revisão da Política	Abril 2024

15. Responsáveis pelo Documento e Aprovações

Atividade	Nome	Nome da área	E-mail
Azimut Brasil WM	Wilson Barcellos	CEO	wilson.barcellos@azimutwealth.com.br
Azimut Brasil WM	Guilherme Doneux	Produtos	guilherme.doneux@azimutwealth.com.br
Azimut Brasil WM	Leonardo Monoli[1]	Gestão	leonardo.monoli@azimutwealth.com.br
Azimut Brasil DTVM	Elisa de Placido[1]	Compliance / Risco	elisa.placido@azimutwealth.com.br
Azimut Brasil DTVM	Marcelo Sepulveda[1]	Operações / Cadastro	marcelo.sepulveda@azimutwealth.com.br

[1]*Diretores Estatutários*