AMB
Wealth

Política de Segurança da Informação

AMB
Wealth

SUMÁRIO

AMB
Wealth

Política de Segurança da Informação

1. Objetivo

O objetivo desta Política de Segurança da Informação ("Política") da AMB Wealth Planner Partners LTDA ("AMB Wealth") é assegurar a proteção de informações, preservando sua confidencialidade, integridade, disponibilidade e autenticidade, em conformidade com a legislação aplicável, normas do mercado financeiro e melhores práticas de governança. Isto se dá através da definição de conceitos claros, da atribuição de diretrizes e responsabilidades, assim como da promoção de uma cultura de conformidade dentro da organização.

Também estão dentre os objetivos desta Política:

- Conscientizar todos os colaboradores sobre a importância de boas práticas de Segurança da Informação, ameaças e riscos;
- Regulamentar o uso e a manutenção das estações de trabalho, equipamentos e periféricos, incluindo, mas não se limitando a desktops, computadores, notebooks, headsets, mouses, teclados, monitores;
- Promover a gestão da Segurança de Informação e minimizar os riscos ligados às informações gerais da AMB Wealth;
- Cumprir requisitos legais e regulatórios, sobretudo, mas sem limitação, à Lei Geral de Proteção de Dados Pessoais (LGPD).

2. Vigência

Esta Política entrará em vigor na data da sua publicação e será revisada a cada dois anos ou quando necessário, devido a alterações regulatórias ou organizacionais, alteração de diretrizes de segurança da informação ou objetivos de negócio.

3. Abrangência

Esta Política se aplica a todos os sócios, diretores, funcionários, estagiários e prestadores de serviço vinculados à AMB Wealth, independentemente do nível hierárquico que atuam em nome da AMB Wealth ("Colaboradores") e que, no

âmbito dessa relação, tenham acesso a áreas, equipamentos, informações, arquivos e dados de propriedade, titularidade ou controle da AMB Wealth.

4. Definições

Informação: define-se informações como os dados organizados e devidamente analisados, que produzem um conhecimento relevante e transmitem um significado gerador de compreensão dentro de um contexto. Podem estar contidas no armazenamento (banco de dados), no tráfego (redes), no processamento e arquivamento, na impressão de documentos, entre outros, através de meios eletrônicos ou físicos.

Informações Confidenciais: entende-se toda a informação material, eletrônica e falada, à qual o colaborador tiver acesso dentro da empresa, incluindo dados da empresa, dos representantes legais, dos associados, de relatórios de órgãos reguladores e do poder público, quando não forem públicos, dados de inspeções e fiscalizações, materiais de marketing e demais informações de propriedade da AMB Wealth.

Informações Sigilosas: são aquelas que possuem proteção legal específica para não serem divulgadas, como bancário, fiscal, industrial, profissional, dados pessoais sensíveis e cuja quebra indevida pode gerar responsabilidade civil, administrativa e penal.

Informações Privilegiadas: qualquer informação relevante a respeito de qualquer sociedade, pessoa ou negócio que envolva AMB Wealth, seus clientes e parceiros, que não tenham sido divulgadas publicamente e que seja obtida de forma privilegiada, em decorrência da relação profissional ou pessoal mantida com um cliente, com colaboradores de clientes ou com terceiros.

Segurança da Informação: refere-se às práticas e medidas adotadas para assegurar a proteção de um conjunto de informações que uma pessoa ou empresa possuem, contra acessos não autorizados, uso indevido, divulgação, alteração ou descarte não autorizado. Tais práticas são orientadas pelos princípios da disponibilidade, integridade, confidencialidade e autenticidade.

Disponibilidade: princípio que garante que as informações estejam disponíveis a pessoas autorizadas sempre que necessário. Para tanto, a AMB Wealth utiliza-se ferramentas como firewall e backup.

Integridade: princípio que garante a veracidade das informações, indicando que os dados mantêm suas características originais e não foram alterados indevidamente. Isso se dá através do estabelecimento de hierarquia de acesso, controle de versões e backups frequentes.

Confidencialidade: princípio que garante a privacidade dos dados, restringindo o acesso de informações da empresa somente a pessoas autorizadas. Para tanto, são utilizadas ferramentas de gestão de acessos, firewall, antivírus e criptografia, a fim de evitar e conter ataques cibernéticos, espionagem, acesso não autorizado, entre outras práticas maliciosas.

Autenticidade: princípio que garante que as informações sejam provenientes de uma fonte confiável, assim como sua autoria. A autenticidade é o pilar que valida a autorização do usuário para acessar, transmitir e receber informações, como logins, senhas, autenticações biométricas ou de dois fatores, assinatura e certificados digitais.

Criptografia: método de codificação das informações, garantidor da confidencialidade, que tem como finalidade evitar que essa seja compreendida por pessoas que não possuem o devido acesso.

Controle de Acessos: é um conjunto de procedimentos e meios utilizados com o objetivo de bloquear ou conceder o acesso às informações a uma pessoa ou grupo de pessoas específico.

Phishing: método que cibercriminosos usam para enganar os alvos, através de envio de e-mails falsos, a fim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros.

Spoofing: método criminoso em que um indivíduo ou sistema falsifica sua identidade ou informações para se passar por outra entidade confiável.

Lei Geral de Proteção de Dados Pessoais (LGPD): Lei nº 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos e digitais, por pessoa física ou jurídica.

Dados Pessoais: são informações que identificam ou tornam possível identificar uma pessoa, como, por exemplo, nome, número de documentos, RG, CPF, endereço, e-mail, endereço de IP, dados fiscais, referências bancárias, dados de pagamento, imagem/fotografia, dentre tantos outros. Podem ser fornecidos pelos titulares ou coletados por meio de bancos de dados públicos.

Dados Sensíveis: são dados pessoais relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso,

filosófico ou político, referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Tratamento de Dados Pessoais: de acordo com a LGPD, é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Colaboradores: todos os profissionais da AMB Wealth, independentemente do nível hierárquico, incluindo sócios, administradores, diretores, funcionários, estagiários, prestadores de serviços e terceiros, como parceiros comerciais, vinculados à empresa.

5. Barreiras da Informação – "Chinese Wall"

Barreiras da Informação consistem no conjunto de procedimentos internos adotados com o objetivo de impedir o fluxo de informações confidenciais, sigilosas e privilegiadas entre setores alheios às atividades, de forma a evitar vazamento de informações, conflito de interesses e práticas fraudulentas.

A AMB Wealth aplica diversas barreiras da informação, dentre as quais destacam-se:

- Controle de acessos com senhas individuais de documentos junto à rede institucional;
- Segregação eletrônica de informações, por área;
- Segregação física dos documentos de cadastro de clientes e de colaboradores.

6. Diretrizes

Se relacionam com essa política o Código de Conduta, o Manual de Compliance e a Política de Privacidade, documentos que possuem objetivos específicos, mas reforçam o compromisso da AMB Wealth com a Segurança da Informação.

Para promover o objetivo desta política, que é a garantia da segurança da informação, são estabelecidas as seguintes diretrizes, que se destinam a todos os colaboradores da AMB Wealth:

6.1. Uso de rede e equipamentos

O uso de equipamentos corporativos e da rede da AMB Wealth é restrito a atividades profissionais, salvo necessária intervenção da área de Tecnologia da Informação.

São práticas obrigatórias a todos os colaboradores:

- Bloquear a tela sempre que se ausentar do posto de trabalho;
- Manter documentos e informações sensíveis fora da visão de terceiros;
- Evitar armazenamento externo não autorizado (pendrives, HDs);
- Não ingerir líquidos ou alimentos sobre equipamentos;
- Desligar ou bloquear equipamentos conforme diretrizes internas;
- Manter sistemas, aplicativos e antivírus atualizados;
- Alterar senhas sempre que solicitado ou diante de suspeita de comprometimento;
- Proteger fisicamente notebooks ou dispositivos móveis da empresa.

6.2. Uso do correio eletrônico

Os sistemas de correio eletrônico (e-mail) devem ser destinados para fins profissionais. De forma geral, é proibido:

- Compartilhar ou enviar mensagens eletrônicas com informações confidenciais, como senhas, detalhes de contas financeiras ou informações pessoais sensíveis, para endereços externos à empresa ou compartilhar informações confidenciais;
- Enviar mensagens eletrônicas com anúncios de eventos particulares, propagandas, opiniões pessoais, vídeos, músicas, campanhas ou promoções;
- Utilizar o e-mail corporativo para participação em fóruns e listas de discussão não relacionados às atividades do usuário na AMB, ou mesmo, utilizar para cadastro em sites de redes sociais, e-commerce, entre outros;

- Transmitir material que seja considerado ofensivo, discriminatório, calunioso, fraudatório, danoso, ilegal ou que possa violar os padrões de ética e cortesia profissional.

Ao abrir um e-mail de um destinatário externo que não pertence ao domínio da AMB Wealth, é importante seguir algumas recomendações para garantir a segurança das informações e evitar possíveis ameaças:

- Antes de abrir qualquer e-mail de um destinatário externo, verifique cuidadosamente o endereço de e-mail do remetente, certificando-se de que seja legítimo e confiável.
- Verifique o formato, gramática e erros de ortografia no e-mail. E-mails de spoofing ou phishing frequentemente apresentam erros ou parecem pouco profissionais. Além disso, observe se o e-mail contém logotipos, imagens ou informações que possam parecer falsas;
- Evite clicar em links dentro de e-mails de remetentes externos, especialmente se você não estiver familiarizado com o conteúdo ou não estiver esperando o e-mail. Se precisar verificar um link, passe o cursor sobre ele para ver o URL completo e certifique-se de que corresponda ao destino esperado.
- Antes de abrir qualquer anexo de um remetente externo, verifique se você estava esperando o arquivo e se o formato é comumente utilizado e considerado seguro.

Lembrando que essas recomendações servem como diretrizes gerais e é importante que, no caso do recebimento de um e-mail que pareça suspeito, o colaborador entre em contato com a equipe de Tecnologia da Informação e relate o incidente.

6.3. Recomendações sobre o uso de senhas

O usuário é o único responsável pelo uso de suas credenciais de acesso. Considerando que a senha é a principal ferramenta de autenticação ou validação de acesso, ela deve ser individual, intransferível e sigilosa, sendo o usuário responsabilizado por qualquer transação efetuada durante o seu uso.

As senhas não devem ser trafegadas em mensagens de e-mail, em sistemas, em aplicativos de mensagens instantâneas, não devem ser anotadas e

ou armazenadas em dispositivos móveis (salvo em aplicativo específico para tal funcionalidade que conte com criptografia forte).

Os sistemas, serviços e dispositivos devem ser configurados para que os padrões mínimos de senha forte sejam exigidos na criação, conforme as recomendações abaixo:

- Uma letra maiúscula;
- Uma letra minúscula;
- Números;
- Símbolos, incluindo: ! @ # $ %^&*-_+=[]{}|\: ‘ , . ?/` ~“<>();
- Tamanho mínimo de 8 caracteres;
- Não utilizar as 3 últimas senhas cadastradas;
- Alterar a senha a cada 180 dias;
- Ativar a verificação de duas etapas.

As solicitações de recuperação de senhas, por esquecimento ou outro motivo, devem ser realizadas pela área de Tecnologia da Informação.

As senhas iniciais devem ser fornecidas diretamente aos usuários e configuradas de forma que, no primeiro acesso, a solicitação de modificação desta ocorra automaticamente.

Ao criar uma senha, evite a utilização de termos, sequências ou caracteres simples, tais como:

- Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família, números de documentos, números de telefone, placa de carros e datas comemorativas;
- Sequência do teclado (ex.: asdfg123);
- Nomes de times de futebol, música, produtos, personagens de filmes, filhos, cônjuge, pais, etc;
- É indicada a utilização de números aleatórios, diferentes tipos de caracteres, caracteres especiais substituição de uma letra por número com semelhança visual.

É importante alterar senhas de acesso sempre que obrigatório ou necessário para fazer cumprir normas de segurança estabelecidas pela AMB Wealth, ou quando haja suspeição de descoberta por terceiros.

Para setores que lidam com acesso a contas bancárias da empresa ou outros sistemas e bancos de dados com informações sensíveis, deve ser utilizada a autenticação multifator.

6.4. Ambiente Físico

Além de manter computadores protegidos por senha, prezando pelo cuidado das informações que é responsável por gerenciar, deve-se manter mesas e locais de trabalho limpos e livres de documentos que contenham informações expostas, evitando a ocorrência de ataques de visual hacking ou shoulder surfing, através da coleta de informações por meios visuais.

Ao utilizar impressoras coletivas, o documento impresso deve ser imediatamente recolhido e, caso não seja mais útil, não deve ser utilizado como folha de rascunho, devendo ser descartado.

Documentos físicos que contenham informações confidenciais e dados pessoais devem ser descartados de forma adequada, através de fragmentação e trituração, quando não houver mais necessidade ou finalidade do tratamento destes pela companhia.

7. Notificação de incidente de segurança

Um incidente de segurança se refere a qualquer evento ou ocorrência que comprometa a segurança das informações, sistemas ou recursos da AMB Wealth.

Um incidente de segurança pode ser:

A. Um acesso não autorizado aos sistemas da empresa;
B. Um acesso não autorizado a dados de outras empresas;
C. Um ataque cibernético aos sistemas da AMB Wealth, com o objetivo de explorar vulnerabilidades e comprometer a segurança da informação;
D. A instalação de arquivos e programas não licenciados;
E. O roubo ou a perda de equipamentos e dispositivos;
F. Desastres naturais ou falhas de infraestrutura, como situações que envolvam incêndio, inundação ou interrupção de energia e/ou rede.

Qualquer vulnerabilidade ou incidente de segurança da informação deve ser imediatamente comunicado ao departamento de Tecnologia da Informação da AMB Wealth, a fim de mitigar os danos, investigar a causa, realizar uma resposta adequada e implementar ações corretivas para evitar futuras ocorrências, sendo vedado ao colaborador a manutenção por empresa ou profissional não autorizado.

8. Sigilo da Informação

Os colaboradores, enquanto estiverem trabalhando na AMB Wealth e mesmo após ter deixado a empresa, devem proteger a confidencialidade de quaisquer informações que não devam ser de domínio público e que foram obtidas durante o exercício de suas funções.

Todas as informações a que o colaborador da empresa tiver acesso, bem como aquelas criadas ou melhoradas durante sua permanência junto à AMB Wealth são de propriedade da empresa e tem caráter confidencial.

A AMB Wealth e seus colaboradores resguardam o sigilo e a confidencialidade das informações pessoais, financeiras e bancárias de seus clientes, aderindo ao disposto na Lei Complementar 105/2001, não sendo, portanto, permitida sua transmissão a terceiros, salvo mediante expressa e prévia anuência do cliente ou exigência legal e/ou judicial.

Todos os colaboradores devem evitar falar sobre clientes, operações, valores e outras questões internas da empresa em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes, etc. Quando se fizer necessária a troca destas informações em locais públicos, deve ser empregada discrição. Perda, mau uso, modificação ou acesso não autorizado a informações sigilosas podem afetar adversamente a privacidade de um indivíduo, desfazer negócios, macular a imagem da empresa e a continuidade de seus negócios.

Caso um colaborador obtenha uma informação confidencial e não necessite utilizá-la, deve comunicar imediatamente à Diretoria de Compliance.

Todas as informações, cópias e extratos são de propriedade da AMB Wealth. Os colaboradores, no término de sua relação com a AMB Wealth, devolverão todos os originais e todas as cópias de quaisquer informações recebidas ou adquiridas, bem como todos os arquivos, correspondências e/ou outras comunicações recebidas, mantidas e/ou elaboradas durante o respectivo contrato.

A divulgação de informações a autoridades governamentais em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada aos sócios da AMB Wealth, para que estes decidam sobre a forma mais adequada para tal.

Tendo em vista a alta especialização da atividade desenvolvida pela AMB Wealth, assim como os princípios que regem o mercado de valores mobiliários, é absolutamente vedada a revelação de carteiras e estratégias de investimento da

AMB Wealth a qualquer não membro da empresa, seja da imprensa, de círculo pessoal de convívio, de ligação imediata de parentesco ou de estado civil.

As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal. Quem tiver acesso a uma informação privilegiada deverá divulgá-la somente a Diretoria de Compliance da AMB Wealth, não devendo divulgá-la a mais ninguém, nem mesmo a outros membros da empresa, profissionais de mercado, amigos e parentes, e nem utilizá-la, em benefício próprio ou de terceiros.

A não observância do sigilo e confidencialidade estará sujeita à apuração de responsabilidades nas esferas cível, administrativa e criminal.

9. Penalidades

É de responsabilidade do usuário o dano que causar pelo descumprimento do disposto nesta Política ou por qualquer outro procedimento de iniciativa própria de tentativa de modificação da configuração, física ou lógica, do computador e/ou rede sem a autorização.

Os profissionais que não observarem os princípios e as regras estabelecidas nesta Política, estão sujeitos a penalidades, podendo acarretar na rescisão contratual entre as partes.

10. Controle de versões

A revisão desta Política será realizada a cada dois anos, podendo ocorrer alterações em períodos menores caso seja identificada, por meio de monitoramento, a necessidade de ajustes nos fluxos, competências, prazos ou na gestão de consequências, entre outros temas.

Versão	Histórico	Data	Área	Elaboração
1	Versão inicial	Agosto de 2023	Compliance	Regina Zanette

2	Revisão de conteúdo	20/08/2025	Compliance	Regina Zanette