Política de Segurança da Informação (Cibernética)

IB Corretora de Câmbio, Títulos e Valores Mobiliários S.A.

Assunto	**Código**
Política	PL022
Documento	**Versão**
Política de Segurança da Informação (Cibernética)	03

Sumário

Assunto	**Código**
Política	PL022
Documento	**Versão**
Política de Segurança da Informação (Cibernética)	03

Quadro Resumo das Revisões

Data	Item	Descrição
Dezembro/2020		Revisada – Sem alterações
Dezembro/2021	**Revisão Geral**	Revogação da Resolução 4.658 de 26 de abril de 2018 pela Resolução nº 4.893 de 26/02/2021

Assunto	Código
Política	PL022
Documento	**Versão**
Política de Segurança da Informação (Cibernética)	03

1. Objetivo

Formalizar os conceitos e as diretrizes da Segurança da Informação (Cibernética) da IB Corretora de Câmbio, Títulos e Valores Mobiliários S.A. (IB) conforme Resolução nº 4.893 de 26/02/2021, do Banco Central do Brasil estabelecendo diretrizes, controles e mecanismos de proteção das informações da organização, para garantir a confidencialidade, integridade e disponibilidade das informações.

2. Abrangência

Aplica-se para todos os colaboradores (funcionários, contratados, terceirizados e trabalhadores temporários), com acesso a qualquer informação, sistema, computador, rede de computadores, ou serviços de informações pertencentes a IB. O cumprimento das diretrizes estabelecidas é fundamental para a efetiva relação de parceria firmada para atingir níveis adequados de proteção à informação.

3. Diretrizes Gerais

a) Deve ser assegurado pelo Departamento de Compliance que esta Política, normas complementares e as responsabilidades quanto à Segurança da Informação (Cibernética) estejam amplamente divulgadas ao público-alvo, visando à sua disponibilidade para todos que se relacionam com a IB e que, direta ou indiretamente, são impactados.

b) Esta Política e suas normas complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, no qual os usuários têm acesso somente aos ativos de informação imprescindíveis para o pleno desempenho de suas atividades. Ou seja, tudo que não estiver expressamente permitido só poderá ser realizado após prévia autorização, devendo ser levado em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

c) A informação deve ser utilizada de forma transparente e apenas para execução de sua atividade profissional.

d) As informações da IB são armazenadas em nuvem em servidor na RTM: Rede de Telecomunicações para o Mercado Financeiro. A Segurança das Informações (Cibernética) é de responsabilidade da empresa, que tem como objetivo orientar aos colaboradores (nos diferentes níveis) nas suas responsabilidades com relação a segurança dos ativos de informação provendo ferramentas que permitam aplicar as melhores práticas de segurança no ambiente físico ou lógico, para garantir o sigilo e a integridade no ciclo de vida da informação, desde a sua recepção, produção, registro, classificação, controle, acesso, manuseio, reprodução, transmissão, guarda e descarte com vistas a minimizar vulnerabilidades, riscos e ameaças a IB.

Os funcionários da IB também entendem o seu papel em relação a segurança da informação como também do sigilo em relação as mesmas.

4. Princípios

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela IB pertence à referida instituição. As exceções devem ser explicitadas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. A IB, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5. Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a IB e/ou terceiros. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores. Todos os dispositivos de identificação utilizados na IB, como as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos (se aplicável), devem estar associados a uma pessoa física e vinculados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas sob qualquer hipótese. É igualmente proibido o compartilhamento de login para funções de administração de sistemas.

6. Computadores e Recursos Tecnológicos

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

• Todos os computadores de uso individual deverão ter senha para restringir os acessos não autorizados.

• Os colaboradores devem informar a gerência qualquer identificação de dispositivo estranho conectado ao seu computador.

• É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico ou por terceiros devidamente contratados para o serviço.

• Deverão ser protegidos por senha (bloqueados), todos os computadores quando não estiverem sendo utilizados.

• Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da IB:

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

• Burlar quaisquer sistemas de segurança.

• Acessar informações confidenciais sem explícita autorização do proprietário.

• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

• Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

7. Responsabilidades

Todos os colaboradores da IB, devem entender qual o seu papel em relação a segurança da informação em suas atividades diárias, também devem conhecer e seguir todas as políticas e procedimentos relacionados a segurança da informação. Quando identificar qualquer incidente de segurança, deve reportá-lo imediatamente para organização e cuidar e proteger as informações.

Para efetuar a gestão dos controles e medidas de Segurança da Informação (Cibernética), a área responsável (RTM), tem um papel estratégico e importante para organização, tem a responsabilidade de definir todas as diretrizes e medias de segurança, buscando evitar ou eliminar riscos e ameaças aos negócios da organização. Deve organizar e orientar os programas de conscientização de segurança juntos a todos os colaboradores.

Os responsáveis pela Segurança da Informação (Cibernética) devem garantir que todas medidas e controles de segurança definidos e implementados, estejam alinhados com as estratégias, normas e legislações vigentes. A RTM testa e avalia os controles e mecanismos de segurança, se os mesmos estão em pleno funcionamento e se os mesmos são suficientes para atender os objetivos.

O Diretor responsável pela política de segurança da informação nomeado junto ao Banco Central do Brasil, é responsável pela política de segurança da informação e pela execução do plano de ação e de resposta a incidentes, com o apoio das demais linhas de defesa da organização.

8. Incidentes de Segurança da Informação

Para efeito desta política, um incidente de segurança é definido como qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação (Cibernética).

9. Controles de Segurança da Informação

Os controles de Segurança da informação, consiste em um conjunto amplo de medidas de segurança, visando minimizar os riscos e ameaças presentes nos ativos de informação. Todos os controles são baseados em boas práticas de segurança adotadas pelo mercado financeiro.

9.1 Princípios da Segurança da Informação (Cibernética)

a) Confidencialidade: garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos (sistemas e ferramentas do pacote Office, como por exemplo Excel) sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

b) Integridade: garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.

c) Disponibilidade: permite que a informação seja utilizada quando necessária, portanto, esteja ao alcance de seus usuários e destinatários e possa ser acessada no momento que for necessário utilizá-la.

9.2 Ciclo de Vida da Informação

Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

a) Manuseio: é a etapa onde a informação é criada e manipulada.

b) Armazenamento: consiste na guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.

c) Transporte: ocorre quando a informação é transportada para algum local, não importando o meio no qual ela está armazenada.

d) Descarte: essa fase refere-se à eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

10. Classificação das Informações

As informações são classificadas em três níveis, Confidencial, Interno e Pública, determinando que elas sejam identificadas e tratadas de acordo com seu nível de importância e classificação.

a) Confidencial: É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da organização.

b) Uso Interno: São informações de nível reduzido de confidencialidade onde qualquer informação que possa ser divulgada a toda a empresa, bem como pessoas vinculadas.

c) Público: São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

11. Gestão de Risco

A gestão dos riscos é realizada através de processos de identificação das vulnerabilidades, ameaças e impactos sobre seus ativos de informação.

Todos os riscos, devem ser identificados, analisados, medidos e se necessário ter o devido plano de ação para seu tratamento e as medidas necessárias para a mitigação ou eliminação dos riscos identificados.

12. Ações de Prevenção e Proteção

Sem prejuízo de ações específicas para proteção e prevenção de riscos identificados e avaliados pela área responsável, são adotadas rotinas padronizadas de prevenção e proteção dos processos e ativos relevantes, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança.

13. Aprovação e Revisão

Esta política é aprovada pela Diretoria e revisada anualmente pela área de Compliance.