
Política da Segurança da Informação

BM&FBOVESPA

A Nova Bolsa



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA BM&FBOVESPA

1. INTRODUÇÃO

A informação é um ativo que possui grande valor para a BM&FBOVESPA, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, *internet*, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

- (i) **Confidencialidade:** somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
- (ii) **Integridade:** somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.
- (iii) **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

Em empresas grandes e complexas, a proteção da informação não é uma tarefa trivial. Em geral, o sucesso da Política de Segurança da Informação adotada por uma instituição depende da combinação de diversos elementos, dentre eles, a estrutura organizacional da empresa, as normas e os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de diretores, funcionários e colaboradores.

2. OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação da BM&FBOVESPA é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores. Seu propósito é estabelecer as diretrizes a serem seguidas pela Bolsa no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

3. ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

3.1. DEFINIÇÃO

A estrutura normativa da Segurança da Informação da BM&FBOVESPA é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- **Política de Segurança da Informação (Política):** constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- **Normas de Segurança da Informação (Normas):** estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- **Procedimentos de Segurança da Informação (Procedimentos):** instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da BM&FBOVESPA.

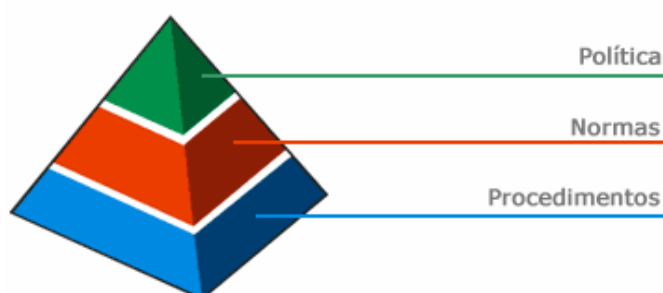


Figura 1 – Estrutura normativa de Segurança da Informação da BM&FBOVESPA.

3.2. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os colaboradores da BM&FBOVESPA e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Os Procedimentos de Segurança da Informação devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

3.3. APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Segurança da Informação da BM&FBOVESPA deverão ser aprovados e revisados conforme os seguintes critérios:

- **Política**
 - Nível de Aprovação: Diretoria Executiva
 - Periodicidade de Revisão: anual
- **Normas**
 - Nível de Aprovação: Comitê Gestor de Segurança da Informação
 - Periodicidade de Revisão: anual
- **Procedimentos**
 - Nível de Aprovação: Diretoria responsável pela área envolvida
 - Periodicidade de Revisão: anual

4. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Cabe a todos os colaboradores (funcionários, estagiários e prestadores de serviços) da BM&FBOVESPA:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da BM&FBOVESPA;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela BM&FBOVESPA;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela BM&FBOVESPA;

- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

Adicionalmente, são definidas as seguintes responsabilidades e atribuições específicas relacionadas à segurança da informação:

4.1. DIRETORIA EXECUTIVA

Em relação à segurança da informação, cabe à Diretoria Executiva:

- Aprovar a Política de Segurança da Informação e suas revisões;
- Aprovar a nomeação dos “proprietários” da informação; e
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação.

4.2. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI)

Cabe ao Comitê Gestor de Segurança da Informação (CGSI):

- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Definir a classificação das informações pertencentes ou sob a guarda da BM&FBOVESPA, com base no inventário de informações apresentado pela Área de Gestão de Segurança da Informação e nos critérios de classificação constantes de Norma específica;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os à Diretoria Executiva, quando for o caso;
- Propor projetos e iniciativas relacionados à melhoria da segurança da informação da BM&FBOVESPA;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Determinar a elaboração de relatórios, levantamentos e análises que dêem suporte à gestão de segurança da informação e à tomada de decisão;
- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação; e
- Propor a relação de “proprietários” das informações da BM&FBOVESPA.

O CGSI terá como membros:

- Diretor Executivo de Operações e TI;
- Diretor de TI – Sistemas de Negociação;
- Diretor de TI – Sistemas de Liquidação, de Depositária e de Risco;
- Diretor de TI – Infra-Estrutura, Arquitetura e Produção;
- Diretor de RH;
- Representante da Diretoria Executiva Financeira, Corporativa e de Relações com Investidores (Diretor Executivo ou Diretor);
- Representante da Diretoria Executiva de Clearings, Depositária e de Risco (Diretor Executivo ou Diretor); e
- Responsável pela área de Gestão de Segurança da Informação.

O Comitê de Auditoria da BM&FBOVESPA poderá, caso queira, indicar representante para participar das reuniões do CGSI na condição de observador/ouvinte.

A coordenação dos trabalhos do CGSI caberá ao responsável pela área de Gestão de Segurança da Informação, cujas atribuições abrangerão a convocação das reuniões e a realização de outros atos de suporte às atividades desenvolvidas.

As reuniões do CGSI:

- (i) Serão realizadas mensalmente, podendo haver convocação em frequência maior ou extraordinariamente, sempre que necessário;
- (ii) Serão instaladas com a presença de, no mínimo, 2/3 (dois terços) dos membros do CGSI; e
- (iii) Deverão ser registradas em ata.

O CGSI deliberará por maioria dos votos presentes.

De acordo com a necessidade, outros profissionais da BM&FBOVESPA e convidados externos poderão participar das reuniões do CGSI.

4.3. ÁREA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Cabe à área de Gestão de Segurança da Informação:

- Convocar, coordenar, lavrar atas e prover apoio às reuniões do CGSI;
- Prover todas as informações de gestão de segurança da informação solicitadas pelo CGSI;

- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores da BM&FBOVESPA;
- Oferecer orientação e treinamento sobre a Política de Segurança da Informação e suas Normas a todos os colaboradores da BM&FBOVESPA;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da BM&FBOVESPA, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso da BM&FBOVESPA, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Analisar os riscos relacionados à segurança da informação da BM&FBOVESPA e apresentar relatórios periódicos sobre tais riscos ao CGSI, acompanhados de proposta de aperfeiçoamento do ambiente de controle da Bolsa, quando for o caso;
- Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações da BM&FBOVESPA;
- Requisitar informações às demais áreas da BM&FBOVESPA (diretorias, gerências, coordenações etc.), realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação; e
- Estabelecer mecanismo de registro e controle de não-conformidade a esta Política e às Normas de Segurança da Informação, comunicando o CGSI.

4.4. PROPRIETÁRIO DA INFORMAÇÃO

O proprietário da informação é um diretor ou um gerente da BM&FBOVESPA, formalmente indicado pela Diretoria Executiva, responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à Bolsa ou sob a sua guarda.

Cabe ao proprietário da informação:

- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da BM&FBOVESPA às autorizações de acesso concedidas;

- Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política e as Normas de Segurança da Informação da BM&FBOVESPA;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
- Analisar os relatórios de controle de acesso fornecidos pela área de Gestão de Segurança da Informação, com o objetivo de identificar desvios em relação à Política e às Normas de Segurança da Informação, tomando as ações corretivas necessárias;
- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

4.5. DIRETORIA JURÍDICA

Cabe à Diretoria Jurídica:

- Manter as áreas da BM&FBOVESPA informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;
- Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da BM&FBOVESPA; e
- Avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da BM&FBOVESPA.

4.6. DIRETORIAS, GERÊNCIAS E COORDENAÇÕES

Cabe às Diretorias, Gerências e Coordenações:

- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Assegurar que suas equipes possuam acesso e conhecimento desta Política, das Normas e dos Procedimentos de Segurança da Informação;

- Redigir os Procedimentos de Segurança da Informação relacionados às suas áreas, mantendo-os atualizados; e
- Comunicar imediatamente eventuais casos de violação de segurança da informação à área de Gestão de Segurança da Informação.

4.7 ÁREA DE RECURSOS HUMANOS

Cabe à área de Recursos Humanos:

- Colher a assinatura do Termo de Responsabilidade dos funcionários e estagiários, arquivando-o nos respectivos prontuários; e
- Informar, prontamente, à área de Gestão de Segurança da Informação, todos os desligamentos, afastamentos e modificações no quadro funcional da empresa.

5. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação da BM&FBOVESPA. Tais diretrizes constituem os principais pilares da Gestão de Segurança da Informação da Bolsa, norteando a elaboração das Normas e dos Procedimentos.

5.1. ADOÇÃO DE COMPORTAMENTO SEGURO

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações da Bolsa, com destaque para os seguintes itens:

- Diretores, gerentes, coordenadores, funcionários e prestadores de serviços devem assumir atitude pró-ativa e engajada no que diz respeito à proteção das informações da BM&FBOVESPA.
- Os colaboradores da BM&FBOVESPA devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.
- Todo tipo de acesso à informação da BM&FBOVESPA que não for explicitamente autorizado é proibido.
- Informações confidenciais da BM&FBOVESPA não podem ser transportadas em qualquer meio (CD, DVD, disquete, *pen-drive*, papel etc.) sem as devidas autorizações e proteções.

- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.).
- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protégido.
- Somente softwares homologados pela BM&FBOVESPA podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de serviços de informática da Bolsa.
- A política para uso de *internet* e correio eletrônico deve ser rigorosamente seguida. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados.
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a área de Gestão de Segurança da Informação.

5.2. ADOÇÃO DE INVENTÁRIO E DE SISTEMA DE CLASSIFICAÇÃO DA INFORMAÇÃO

A área de Gestão de Segurança da Informação deve manter um inventário atualizado que identifique e documente a existência e as principais características de todos os seus ativos de informação (base de dados, arquivos, diretórios de rede, trilhas de auditoria, códigos fonte de sistemas, documentação de sistemas, manuais, planos de continuidade etc.).

As informações inventariadas devem ser classificadas de acordo com o grau de confidencialidade e criticidade para o negócio da BM&FBOVESPA, e com base na Norma de classificação de informações estabelecida pela Bolsa.

As informações inventariadas devem ser associadas a um “proprietário”, o qual é um diretor ou um gerente da BM&FBOVESPA, formalmente designado pela Diretoria Executiva como responsável pela autorização de acesso às informações sob a sua responsabilidade.

5.3. AVALIAÇÃO CONTÍNUA DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO

A área de Gestão de Segurança da Informação deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação da BM&FBOVESPA.

A análise dos riscos deve atuar como ferramenta de orientação ao Comitê Gestor da Segurança da Informação, principalmente, no que diz respeito à:

- Identificação dos principais riscos aos quais a informação da Bolsa está exposta; e
- Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas etc.

O escopo da análise/avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.

5.4. GESTÃO DE ACESSO A SISTEMAS DE INFORMAÇÃO E A OUTROS AMBIENTES LÓGICOS

Todo acesso às informações e aos ambientes lógicos da BM&FBOVESPA deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação.

A política de controle de acesso deve ser documentada e formalizada por meio de Normas e Procedimentos que contemplem, pelo menos, os seguintes itens:

- Procedimento formal de concessão e cancelamento de autorização de acesso a usuário aos sistemas de informação;
- Comprovação da autorização do proprietário da informação;
- Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;
- Verificação se o nível de acesso concedido é apropriado ao propósito do negócio e se é consistente com a Política de Segurança da Informação e suas Normas;

- Remoção imediata de autorizações dadas a usuários afastados ou desligados da empresa, ou que tenham mudado de função;
- Processo de revisão periódica das autorizações concedidas; e
- Política de atribuição, manutenção e uso de senhas.

5.5. MONITORAÇÃO E CONTROLE

Os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da BM&FBOVESPA, não podendo ser interpretados como de uso pessoal.

Todos os profissionais e colaboradores da BM&FBOVESPA devem ter ciência de que o uso das informações e dos sistemas de informação da Bolsa pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

6. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.