**M.P12.001.05**

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
# TI - TECNOLOGIA DA INFORMAÇÃO

## 1. Introdução

A Mirae Asset Wealth Management entende que a informação é um dos principais ativos da empresa ou confiados a ela, portanto preza pela adequada utilização e proteção contra qualquer tipo de risco ou ameaça.
Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, não estando esta segurança restrita somente a informações eletrônicas, sistemas de armazenamento ou documentação impressa disponível. O conceito se aplica a todos os aspectos de proteção de informações e dados.
A proteção existente sobre as informações de uma determinada empresa ou pessoa é chamada de segurança da informação, portanto aplica-se tanto para informações corporativas quanto para informações pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.
A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação. 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, verbal, em mídias de áudio e de vídeo, etc.
A adoção de políticas e procedimentos que visem garantir a segurança da informação é prioridade constante da empresa, por meio delas, a Mirae Asset Wealth Management procura reduzir os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da instituição.

## 2. Objetivo

Este documento não tem por objetivo descrever os aspectos técnicos de implementação dos mecanismos de segurança, mas sim apresentar de forma resumida os principais recursos utilizados pela empresa para garantir a segurança da informação em seus diversos níveis, bem como conscientizar os colaboradores e demais partes interessadas que possam ter acesso às informações da empresa quanto à importância no tratamento das informações e a forma com que a Mirae Asset Wealth Management conduz essa questão.
A Política de Segurança da Informação ora apresentada visa instituir um nível de segurança adequado às características da empresa e foi desenvolvida com base nos

resultados de análises dos riscos associados ao negócio, nos atributos de segurança, na estrutura física, tecnológica e humana disponível na corretora.
A composição de segurança de informação adotada pela empresa é constituída de procedimentos (documentados ou não), capacitação de colaboradores, controles de acessos físicos e lógicos, procedimentos e controles de recursos humanos e respectiva interação com demais processos, disciplina e atividades da área de Tecnologia da Informação, verificação e testes pelas áreas de Controles Internos & Compliance, dentre outras atividades de menor relevância inerentes aos processos de uma corretora de valores.

## 3. Atribuições e responsabilidades

É dever de todos os colaboradores (Diretores, funcionários, prestadores de serviços, estagiários e trainees):

- Cumprir fielmente a Política e demais regulamentos internos e externos relacionados a Segurança da Informação;
- Buscar orientação do superior hierárquico ou da área de Controles Internos & Compliance em caso de dúvidas relacionadas à segurança da informação;
- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela empresa;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades inerentes a função desempenhada;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente à área de Controles Internos & Compliance qualquer descumprimento ou violação desta Política ou suspeita de manipulação inadequada de informações.

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

### 3.1 Área de Controles Internos & Compliance

- Desenvolver a Política de Segurança da Informação e suas revisões;
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política ou situações similares, submetendo, se necessário, ao Diretor de Compliance;

- Prover ampla divulgação da Política e demais controles de Segurança da Informação para todos os colaboradores da empresa;
- Analisar os riscos relacionados à segurança da informação e propor ações se necessário;
- 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

### 3.2 Diretoria

- Aprovar a Política de Segurança da Informação e suas revisões;
- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor projetos e iniciativas relacionados à melhoria da segurança da informação;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Incentivar a cultura de controles e a disciplina na utilização das informações.

### 3.3 CEO

- Estabelecer procedimentos e definir diretrizes dos controles de acessos;
- Analisar os riscos relacionados à segurança da informação e propor ações se necessário

### 3.4 Gestores das áreas

- Auxiliar a área de Controles Internos & Compliance (Proprietário da Informação) no estabelecimento das autorizações de acesso às informações;
- Fomentar junto à equipe sob sua gestão a cultura de controles e a adequada utilização das informações;
- Cumprir e fazer cumprir esta Política e demais procedimentos de Segurança da Informação;
- Assegurar que suas equipes possuam acesso e conhecimento desta Política, bem como os conceitos que a cercam;
- Comunicar imediatamente eventuais casos de violação de segurança da informação à área de Controles Internos & Compliance.

### 3.5 Área de Recursos Humanos

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

### 3.6 Área de Tecnologia da Informação

- Operacionalizar os acessos definidos pela área de Controles Internos & Compliance em conjunto com RH e a própria TI;
- Oferecer orientação e treinamento sobre a Política de Segurança da Informação e assuntos relacionados;
- Manter-se atualizada em relação às melhores práticas existentes no mercado em relação às tecnologias disponíveis;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso da empresa, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Analisar os riscos relacionados à segurança da informação da empresa e apresentar relatórios periódicos sobre tais riscos;
- 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 empresa, apresentando proposta de aperfeiçoamento quando necessário;
- Realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e demais procedimentos relacionados à Segurança da Informação;
- Estabelecer mecanismo de registro e controle de não-conformidade a esta Política e demais procedimentos de Segurança da Informação, comunicando a área de Controles Internos & Compliance;
- Participar da investigação de incidentes de segurança relacionados à proteção de informações.

## 4. Atributos da Segurança da Informação

O trio Confidencialidade, Integridade e Disponibilidade representa os principais atributos que orientam a análise, o planejamento e a implementação da segurança das informações contidas ou disponíveis na empresa, para tanto descrevemos a seguir os conceitos desses atributos para melhor entendimento:

Confidencialidade – propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
Integridade – propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças (registros) e garantia do seu ciclo de vida (criação, manutenção e destruição).
Disponibilidade – propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas três características principais, quais sejam:

Perda de Confidencialidade: seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo com que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.
Perda de Integridade: aconteceria quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.
Perda de Disponibilidade: acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como crackers, (hackers não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas). Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, auto-estima, vingança e o dinheiro.

## 5. Mecanismos de Segurança

Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação) que a suporta.

Existem mecanismos de segurança que apoiam os controles físicos, como: Portas / trancas / paredes / blindagem / guardas / etc...

Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.
Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os anti-vírus, firewalls, firewalls locais, filtros anti-spam, fuzzers, analisadores de código, etc. Dentre os principais mecanismos de segurança que apóiam os controles lógicos destacamos: criptografia, assinatura digital, palavras e senhas de acesso.

## 6. Diretrizes

Apresentamos a seguir as principais diretrizes da Política de Segurança de Informação da Mirae Asset Wealth Management. Essas diretrizes devem ser de conhecimento de todos os colaboradores da empresa e deverão ser seguidas em sua íntegra, sendo esperado um comportamento responsável e diligente em todos os níveis hierárquicos da empresa, bem como para todos os processos inerentes às atividades da corretora.

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, especialmente quanto aos 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;
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos. Entende-se por adequadamente armazenados e protegidos a utilização de armários com trancas, controles de acesso eletrônico ou físico de qualquer natureza, trancamento do ambiente de trabalho entre outros controles que impeçam o acesso à informação;
- Os colaboradores da Mirae Asset Wealth Management 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 empresa que não for explicitamente autorizado é proibido;
- Informações confidenciais da empresa 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-protegido;
- Somente softwares homologados pela Área de Tecnologia da Informação podem ser instalados nas estações de trabalho e devem ser por ela executadas;
- O uso de internet e correio eletrônico devem ser feitos de forma cuidadosa e com bom senso. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados;
- É expressamente proibida a utilização de aparelhos celulares nos ambientes de operações da corretora;
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação deve ser imediatamente esclarecido com a área de Controles Internos & Compliance.

## 7. Nível de segurança

Com base na análise dos riscos e ameaças inerentes à Segurança da Informação em uma instituição financeira, mais especificamente uma Corretora de Valores, a Mirae Asset Wealth Management definiu o nível de segurança necessário para a proteção das informações e a condução de seu negócio de acordo, não só com a regulamentação vigente, como também com as melhores práticas do mercado, para tanto foram consideradas:

Segurança Física: Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, acesso indevido de pessoas, forma inadequada de tratamento e manuseamento do material.

Segurança Lógica: Considera mecanismos contra ameaças ocasionadas por vírus, acessos remotos à rede, backup desatualizados, violação de senhas, etc.

Foram considerados ainda, como objetivos da política de segurança da informação, a garantia dos seguintes elementos:

- A Disponibilidade: o sistema deve estar disponível de forma que quando o usuário necessitar possa usar. Dados críticos devem estar disponíveis ininterruptamente;
- A Utilização: o sistema deve ser utilizado apenas para os determinados objetivos;
- A Integridade: o sistema deve estar sempre íntegro e em condições de ser usado.
- A Autenticidade: o sistema deve ter condições de verificar a identidade dos usuários, e este, condições de analisar a identidade do sistema.
- A Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado.

## 8. Política de Senhas

Para a definição da política de senhas da Mirae Asset Wealth Management a área de Tecnologia da Informação em conjunto com Controles internos & Compliance ponderou as principais ameaças e eventuais desconfortos que a empresa e seus colaboradores estariam suscetíveis.

Portanto foram adotadas as seguintes regras:

- Período de expiração
  Fica definido o prazo de validade de no máximo 45 dias, sendo o usuário obrigado a renovar a senha durante esse período.

- Composição da senha
  Obrigatoriedade de no mínimo 8 caracteres, sendo que deve ser atendida pelo menos 3 condições de 4 apresentadas (Caixa baixa, Caixa Alta, Números e caracteres especiais). Qualquer sequência dessas condições são aceitas como uma senha válida desde que atenda a pelo menos 3 condições.

- Senhas que não podem ser utilizadas
  É mantida pela área de Tecnologia da Informação uma base de dados com formatos conhecidos de senhas que verifica e proíbe o seu uso, como por exemplo: o usuário chama-se Jose da Silva, logo sua senha não deve conter partes completas do nome como 12!@jose ou 12!@silva etc, porém partes de seu nome são aceitos como 12!@jos ou 12!@sil etc.

- Histórico de Senhas
  A nova senha não pode ser igual as ultimas 6 senhas. Sendo assim nossos sistemas armazenam as últimas 6 senhas de cada usuários (em banco de dados que suporte criptografia de dados) e essas não poderão ser utilizadas.

- Bloqueio de senha
  Caso uma senha seja digitada de forma errada mais de duas vezes em um intervalo de 30 minutos a senha do usuário será BLOQUEADA e somente o departamento de TI poderá reativar a conta, após abertura de chamado formal.

Cabe ressaltar que, tão importante quanto às regras definidas para o uso das senhas, é a conscientização de todos os colaboradores quanto à correta utilização e as responsabilidades implícitas no conhecimento das mesmas.

## 9. Política de Backup

A área de Tecnologia da Informação da Mirae Asset Wealth Management é responsável por operacionalizar rotina de backup para todos os arquivos abaixo relacionados:

- Servidor de Arquivos;
- Caixas de e-mails;
- Banco de Dados de Sistemas;
- Arquivos de configurações de equipamentos de redes;
- Gravações de todas as ligações telefônicas da empresa;
- Histórico de todas as conversas em Instant Messengers autorizados;

Os backups abaixo relacionados são realizados em mídia descartável com validade de mais de 10 anos (unidade de fita como DAT e LTO) e armazenados em local seguro e com acesso controlado.

A rotina de backup segue o seguinte cronograma:
Diariamente: Backup Incremental (Contenção Semanal – Salvaguarda*)
Semanalmente: Backup Full (Contenção Mensal – Salvaguarda*)
Mensalmente: Backup Full (Contenção Quinquanual – Salvaguarda*)

*Salva Guarda
Uma cópia da mídia de backup é duplicada e enviada a um local seguro, a uma distância de mais de 10 Kilometros. Utilizamos o serviço de Custódia e Salvaguarda de Mídias da empresa Iron Mountain. Assim a Iron Mountain é o fornecedor responsável pelo armazenamento dessa segunda cópia de segurança além da logística de transporte das mídias.

## 10. Gestão de acessos

Todo controle de acessos aos ambientes físicos e lógicos da Mirae Asset Wealth Management é definido pela área de Controles Internos & Compliance (Proprietário da Informação), em conjunto com as áreas de Recursos Humanos e Tecnologia da Informação, sendo esta última a responsável pela viabilização dos acessos e o controle da conformidade das liberações com os perfis definidos.

Os controles definidos para a gestão dos acessos contemplam os seguintes itens:

- Descritivo de concessão, alteração e cancelamento de acesso;
- Requerimento para Concessão de Acessos (Apêndice A);
- Termo de compromisso para com a Política de Segurança da Informação;
- Matriz de Acessos que visa garantir que o acesso concedido é apropriado à função do profissional (Apêndice B);
- Processo de revisão periódica dos acessos concedidos.

### 10.1 Descritivo de concessão

Para novos colaboradores a área de Recursos Humanos comunica a contratação por e-mail a área de Tecnologia da Informação, descrevendo o cargo e a função que o colaborador irá ocupar. De posse da informação a área de Tecnologia da Informação verifica se a função do novo colaborador já se encontra contemplada na Matriz de Acessos e viabiliza acessos conforme documento.
Caso a função do novo colaborador não esteja contemplada na matriz, a área de Controles Internos & Compliance deverá ser contatada para auxiliar na definição dos acessos.

### 10.2 Descritivo de alterações de acessos

As alterações de perfis de acessos ou novos acessos a colaboradores das áreas devem ser solicitadas pelos gestores do respectivo colaborador por meio de e-mail à área de Tecnologia de Informação que, caso o acesso ainda não esteja contemplado na matriz de acessos deve submeter à autorização da área de Controles Internos & Compliance.

### 10.3 Descritivo de bloqueio e cancelamento de acessos

Bloqueios e cancelamentos de acessos são efetuados a pedido da área de Recursos Humanos, quando do desligamento de profissionais ou pela área de Controles

Internos & Compliance, para o cumprimento de regulamentações ou com foco na mitigação de riscos. Em ambos os casos a solicitação deve ser feita por meio de e-mail direcionado para área de Tecnologia da Informação, que deve guardar o documento como forma de registro.

## 11. Monitoramento e eventuais sanções

Os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da Mirae Asset Wealth Management, não podendo ser considerados ou interpretados como de uso pessoal.
Todos os profissionais e colaboradores da empresa devem ter ciência de que o uso das informações e dos sistemas de informação da Mirae pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política de Segurança da Informação de demais controles relacionados e, conforme o caso poderá servir como evidência em processos administrativos e/ou legais.

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

## 12. Guarda de Registros

| Identificação | Armazenamento | Proteção | Recuperação | Tempo de retenção | Descarte |
|---|---|---|---|---|---|
| Matriz de acessos | Eletrônico | Diretório com Acesso Restrito | Documento único | Permanente | ------ |
| Requerimento para Concessão de Acessos | Documento Digitalizado | Diretório com Acesso Restrito | Cronológica | 3 anos | Deletar |

## Apêndice A - Requerimento para Concessão de Acessos

| MIRAE ASSET Building on principles | Requerimento para Concessão de Acessos | June 15, 2010<br>F.P12.001.01 |
|---|---|---|

1. Identificação:

| Motivo da solicitação: | Tipo de vínculo<br>*Ex. CLT, terceiro, auditor, consultor* |
|---|---|
| Nome da pessoa que pretende ter o acesso | Cargo / Função |
| Nome do gestor responsável | Cargo / Função do Gestor |

2. Informações do acesso:

| Acesso pretendido<br>*Especificar o(os) sistema(s) ou ambiente(s) objeto deste requerimento.* | Tipo de acesso a ser concedido<br>Caso as opções abaixo não mencionem o tipo de acesso desejado, descrever abaixo : |
|---|---|
| | ☐ Total ☐ Apenas Consulta ☐ Supervisor ☐ Negociação |
| | ☐ Total ☐ Apenas Consulta ☐ Supervisor ☐ Negociação |
| | ☐ Total ☐ Apenas Consulta ☐ Supervisor ☐ Negociação |
| | ☐ Total ☐ Apenas Consulta ☐ Supervisor ☐ Negociação |
| | ☐ Total ☐ Apenas Consulta ☐ Supervisor ☐ Negociação |

3. Lista de aprovações:

| Solicitante | Cargo/ Função | Assinatura |
|---|---|---|
| Superior Imediato (Gestor) | Cargo/ Função | Assinatura |
| Controles Internos & Compliance | Cargo/ Função | Assinatura |
| Tecnologia da Informação | Cargo/ Função | Assinatura |

Importante:

Os acessos físicos e a sistemas da empresa devem ser concedidos com base no princípio do privilégio mínimo, ou seja, apenas os acessos necessários ao desempenho das funções inerentes ao cargo do colaborador devem ser requisitados.

Atenção: Os acessos e senhas são de uso pessoal e intransferível, nunca divulgue a ninguém.

, de de de 20.

## Apêndice B – Matriz de Acessos

| ACESSOS \ CARGOS | | Administrador de Banco de Dados (DBA) | Advogado | Agente Autônomo de Investimento | Analista de Back Office | Analista Contábil | Analista de Cadastro | Analista de Clubes e Fundos | Analista de Custódia - Bovespa | Analista de Rede | Analista de Gestão de Fortunas | Analista de Gestão de Fortunas Junior | Analista de Operações |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Físico | Porta Principal | | | | | | | | | | | | |
| | Custódia | | | | | | | | | | | | |
| | Call Center (atendimento) | | | | | | | | | | | | |
| | Mesa de Operações | | | | | | | | | | | | |
| | CPD | | | | | | | | | | | | |
| | Gestão de Recursos de Terceiros | | | | | | | | | | | | |
| Operacional | Megabolsa | | | | | | | | | | | | |
| | Bloomberg | | | | | | | | | | | | |
| | Broadcast | | | | | | | | | | | | |
| | GTS | | | | | | | | | | | | |
| | RMS (Risk Management System) | | | | | | | | | | | | |
| | Fast Trader (DMA 1) | | | | | | | | | | | | |
| | Robotrader (DMA 1) | | | | | | | | | | | | |
| | SELIC | | | | | | | | | | | | |
| | CETIP | | | | | | | | | | | | |
| | SISBACEN | | | | | | | | | | | | |
| Controle | Controle de Risco (Sisfinance) | | | | | | | | | | | | |
| | Clubes e Fundos - SIM Online | | | | | | | | | | | | |
| | Administrativo Site Mirae | | | | | | | | | | | | |
| | Módulo Admin Marketing - Site | | | | | | | | | | | | |
| | Renda Fixa / Minicon | | | | | | | | | | | | |
| SINACOR | Acompanhamento Controle | | | | | | | | | | | | |
| | Apuração Resultados | | | | | | | | | | | | |
| | BTC | | | | | | | | | | | | |
| | Cadastro | | | | | | | | | | | | |
| | Conta Corrente | | | | | | | | | | | | |
| | Controle - Acessos | | | | | | | | | | | | |
| | Controle - Mensageria | | | | | | | | | | | | |
| | Contas a Pagar | | | | | | | | | | | | |
| | Custódia | | | | | | | | | | | | |
| | DataBase - Marketing | | | | | | | | | | | | |
| | Faturamento - BM&F | | | | | | | | | | | | |
| | Faturamento - Bovespa | | | | | | | | | | | | |
| | GAB | | | | | | | | | | | | |