1. OBJETIVO

1.1 Este documento fornece informações à equipe de trabalho da ORIA GESTÃO DE RECUROS ("ORIA"), de forma a orientá-la quanto aos cuidados legais exigidos no que se refere a Segurança da Informação.

1.2 Assegurar controles adequados na gestão da informação e alertar e informar todos os funcionários para que estejam treinados e preparados.

2. CONCEITO

2.1 A Segurança da Informação se refere à proteção existente sobre as informações da gestora e de seus clientes.

2.2 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.

2.3 ORIA, em sua política, definiu adotar os seguintes atributos básicos, em conformidade com as melhores práticas de mercado:

2.4 Confidencialidade - limitar o acesso à informação tão somente às entidades legítimas, ou seja, aquelas autorizadas pelo proprietário da informação.

2.5 Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

2.6 Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

3. RISCOS

3.1 Os riscos que podem advir da ausência de controles adequados são:

3.2 Perda de Confidencialidade: 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.

3.3 Perda de Integridade: 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 da informação.

3.4 Perda de Disponibilidade: quando a informação deixa de estar acessível para quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceria com a queda de um servidor, ou de uma aplicação crítica de negócio, que apresentasse 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.

4. MECANISMOS DE SEGURANÇA

4.1 Senhas de acesso físico: Todos os funcionários deverão gerar senhas individuais de acesso para o porteiro eletrônico, conforme procedimentos distribuídos pela Gerencia Administrativa. As senhas criadas são individuais e intransferíveis. No caso do desligamento de qualquer funcionário, o gestor administrativo será o responsável por desativar o acesso do mesmo imediatamente após o seu desligamento.

4.2 Controle e guarda de documentos físicos: Os documentos físicos caracterizados como de acesso restrito e de caráter sigiloso são guardados em local fechado e com acesso restrito somente às pessoas autorizadas:

- Controle de depósito e retirada de documentos restrita aos funcionários da ORIA.

- A disponibilidade dos documentos deve ser garantida por processo criterioso desde o momento do arquivamento, critérios de localização adequados entre outros processos considerados necessários.

São considerados documentos de acesso restrito e caráter sigiloso:

I. Demonstrativos financeiros;

II. Contratos com partes terceiras;

III. Contratos, atas e demais documentos societários

4.3 Controle de acesso aos sistemas e repositórios online: A ORIA não utiliza redes internas ou máquinas virtuais eliminando um ponto adicional de vulnerabilidade no seu controle da segurança da informação. A empresa acredita que a segurança da informação garantida em aplicações, sistemas e repositórios de arquivos online entregues no modelo de software como serviço (Software as a Service), nos quais grandes fornecedores como por exemplo Salesforce.com Inc. (NYSE:CRM) possuem investimentos e especialização em segurança da informação com ordem de grandeza infinitamente maior do que uma gestora de recursos pode ter.
O acesso a esses sistemas da ORIA é controlado e limitado aos seus colaboradores. O acesso se dá por usuário, com diferenciação de perfil de acesso (segregação de funções) através de senha. A senha é pessoal e intrasferível e inclui mecanismos de verificação dupla via sms ou email.
Qualquer alteração ou autorização de acesso deverá ser enviada ao responsável de TI com cópia para o responsável de Compliance.
O responsável de TI, realiza monitoramento pontual à utilização dos sistemas da ORIA por seus usuários a fim de identificar acessos indevidos e garantir a segurança das informações registradas nesses sistemas.

4.4 A utilização de programas de correio eletrônico ou “e-mails” deve ser exclusivamente para mensagens de âmbito profissional, pois carregam a identificação da empresa para o ambiente da rede mundial de computadores. Em hipótese alguma, esses sistemas de troca de mensagens devem ser utilizados para transmitir ou retransmitir mensagens que possam comprometer o nome da ORIA, principalmente as que carreguem textos ou anexos que possam ser qualificados como ofensivos.

4.5 Não é permitida a utilização de e-mails particulares (tais como, GMAIL, Terra, UOL, etc.) para o uso corporativo.

4.6 Os sistemas computacionais móveis da ORIA devem ser utilizados exclusivamente para as atividades profissionais para as quais o funcionário, foi contratado. Na categoria de sistemas computacionais móveis incluem-se notebooks, modems, sistemas de telefonia inteligentes (smartphones) e tablets.
Em todos os dispositivos de computação móvel não devem ser instalados, processados ou utilizados quaisquer outros denominados “sistemas aplicativos” ou “programas de software” que não tenham a devida licença autorizada ou mesmo a devida homologação concedida formalmente pela ORIA.

4.7 A inclusão de perfis nos sistemas de gestão da ORIA qualifica o usuário para a utilização de todos os recursos dos sistemas autorizados pelo Administrador de Sistemas e pela Gerência a qual está subordinado o usuário. A partir de sua inclusão, o usuário estará automaticamente subordinado às regras de utilização da ORIA.

4.8 A Gerência, a qual está subordinada o usuário, é responsável pela definição das atribuições, das autorizações, manutenções, suspensões ou cancelamento definitivo de perfis junto ao Administrador do Sistema.

4.9 Todos os funcionários deverão, quando ausentar-se de sua estação de trabalho, efetuar o bloqueio da mesma, visando medidas de segurança e redução no consumo de energia. Entende-se por ausentar-se o fato de deixar a estação de trabalho, independente da razão ou do tempo, sem monitoramento pessoal de cada usuário.

4.10 Todos os documentos gerados nos processos internos da ORIA são considerados como confidenciais, devendo-se evitar a divulgação indevida de quaisquer informações contidas nos mesmos.

4.11 Para assegurá-la a confidencialidade das informações impressas, estas serão fragmentadas para impedir sua leitura.

4.12 A ORIA não processa internamente nenhum aplicativo relacionado ás rotinas da empresa. Nos contratos aonde venham envolver o processamento de dados confidencias, deverão ser incluídas cláusulas que tratem dos cuidados necessários para o tratamento confidencial destas informações coobrigando as contrapartes da ORIA ao cumprimento desta Política.

4.13 A ORIA possui um Administrador de Sistemas alocado com a missão de assegurar o mais eficiente suporte às necessidades dos processos de geração de negócios. Semanalmente é enviado ao responsável por Compliance relatório de monitoramento de T.I.

5. SIGILO DE INFORMAÇÕES

5.1 Cumprir as determinações BACEN no MNI-02-01-14 que trata do sigilo bancário que especifica:
"As sociedades corretoras de títulos e valores, e as sociedades distribuidoras de títulos e valores mobiliários devem conservar sigilo em suas operações e serviços prestados, só revelando mediante autorização dos clientes, por escrito." (Res. 38 XII b, Res.1120 RA. Art13, Res.1655 RA art.13, e Res.170 RA art.10).
O nome e as operações do Comitente devem ser informados por ordem ou pedido escrito do Banco Central, da CVM, das Bolsas de Valores ou de autoridades judiciais, dentro dos casos previstos na legislação em vigor.

5.2 Áreas de aplicação:

a) Para todos os colaboradores da ORIA.

b) Para o distribuidor contratado para distribuir os fundos sob a gestão da gestora.
c) Para o agente autônomo contratado para distribuir os fundos sob gestão da gestora.

d) Para ex-colaboradores que terão por obrigação cumprir os termos constantes desta política por prazo aqui estabelecido assim como quando era um colaborador ativo da ORIA.

5.3 Na distribuição de fundos a clientes: para minimizar os riscos de imagem, uma vez que os clientes podem vincular o nome do gestor a uma eventual falha que possa ocorrer em suas informações, recomenda-se que os gestores discutam a Política de Privacidade dos distribuidores, com os quais venha disponibilizar seus fundos e que seja tratado nos contratos de distribuição a garantia de privacidade dos clientes que vierem a adquirir os fundos geridos pela ORIA.

5.4 No dia-a-dia:
Os funcionários durante a permanência em funções de confiança na ORIA, e mesmo após ter deixado a empresa, devem proteger a confidencialidade de quaisquer informações que não devem ser de domínio público. Informações essas que foram obtidas durante o exercício de suas funções como membro da ORIA.
Dentre essas informações encontram-se informações que não devem ser de domínio público, são elas:

- Operações, estratégias, resultados, ativos, dados e projeções que possam levar a uma vantagem competitiva da Gestora frente a seus concorrentes;

- Informações sobre o plano de negócios da empresa;

- Informações confidenciais sobre os funcionários da empresa; e

- Informações sobre clientes, distribuidores e fornecedores.

Questões delicadas envolvendo assuntos da Gestora não devem ser discutidas em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes, etc.
O e-mail interno da empresa é controlado, e as mensagens podem ser rastreadas pelo diretor responsável pelo Compliance em caso de suspeita de qualquer infração relacionado com as Políticas, Normas e Procedimentos da Gestora.

5.5 Para ex-colaboradores:

Não é permitido ao ex colaborador, pelo prazo de 2 anos, utilizar das informações obtidas durante o exercício de suas atividades na ORIA, de qualquer teor, sendo estas informações sigilosas ou não, em benefício próprio ou por qualquer outra razão, ainda que em benefício da própria ORIA.
Caso seja de conhecimento da ORIA da ocorrência, pelo ex funcionário, do vazamento de informações sigilosas ou tentativa de manchar a imagem da companhia perante os clientes, no intuito de torná-lo ex cliente, o profissional poderá responder criminalmente e civilmente pelos seus atos.

5.6 Da mesma forma, funcionários ou colaboradores devem evitar manter em suas mesas papéis e documentos confidenciais. Documentos confidenciais devem ser guardados em local apropriado e com chave, mesmo no decorrer do expediente para evitar o acesso de terceiros não autorizados. Ao final do dia, as mesas devem permanecer sem papéis ou documentos.

5.7 Segurança de TI: ponto adicional de vulnerabilidade no seu controle da segurança da TI. A empresa acredita que a segurança da TI garantida em aplicações, sistemas e repositórios de arquivos online entregues no modelo de software como serviço (Software as a Service), nos quais grandes fornecedores como por exemplo Salesforce.com Inc. (NYSE:CRM) possuem investimentos e especialização em segurança da informação com ordem de grandeza infinitamente maior do que uma gestora de recursos possa ter.

5.8 O acesso a esses sistemas da ORIA é controlado e limitado aos seus colaboradores. O acesso se dá por usuário, com diferenciação de perfil de acesso (segregação de funções) através de senha. A senha é pessoal e intrasferível e inclui mecanismos de verificação dupla via sms ou email.

5.9 Qualquer alteração ou autorização de acesso deverá ser enviada ao responsável de TI com cópia para o responsável de Compliance.

5.10 O responsável de TI, realiza monitoramento pontual à utilização dos sistemas da ORIA por seus usuários a fim de identificar acessos indevidos e garantir a segurança das informações registradas nesses sistemas.
Os links de internet são redundantes, contando com a conexão via NET de 20 Mbps e Vivo 60Mbps.

5.10 A empresa faz uso de anti-spam para bloquear mensagens de e-mails mal-intencionadas, a utilização é vinculada ao sistema da própria Microsoft e tecnologia Exchange online que faz o rastreamento das entradas e saídas dos e-mails no servidor de internet.

5.11 O firewall da ORIA é baseado em iptables que bloqueia acessos indevidos à rede através do sistema SuSE-Firewall System.

5.12 Como software de antivírus principal, a empresa faz o uso do Microsoft Security Essentials. O software é atualizado diariamente e de forma automática, o mesmo executa varreduras semanais na busca de softwares que possam comprometer toda a estrutura de TI da empresa.

6. QUADRO DE REVISÕES

Nº	MOTIVO DA REVISÃO	DATA
0	Emissão inicial	02/06/16

LISTA DE TREINAMENTO

Colaborador	Data	Assinatura

São Paulo, de de 20

Assinatura do Instrutor:
Nome: