Política de Segurança de Informação

Confidencialidade, Disponibilidade e Integridade

Área de Gestão de Compliance

Versão 1.4

I – Controle de Versão

Versão	Data	Nome	Ação (Elaboração, Revisão, Alteração)	Conteúdo
1.0	27/05/2016	Iguana Consultoria	Elaboração	Primeira versão do documento.
1.1	15/06/2016	Iguana Consultoria	Alteração	Ajustes de acordo com a reunião de 10/06 com o Paulo Medeiros.
1.2	29/06/2016	Iguana Consultoria	Alteração	Preparação do documento para upload no site.
1.3	25/06/2017	Iguana Consultoria	Revisão	Revisão anual
1.4	12/04/2018	Iguana Consultoria	Revisão	Revisão anual
	02/05/2018	Diretoria EuvCapital	Aprovação	

II – Sumário Executivo

Objetivos da Política:

- Proteger os nossos clientes, a imagem da **EuvCapital** e as informações pertencentes a ambos;
- Garantir a continuidade do negócio de forma que não haja interrupção dos serviços prestados a nossos clientes e reduzir as perdas em uma situação de acionamento da contingência;
- Reduzir os riscos com fraudes, espionagens, sabotagem, vandalismo, problemas causados por vírus, erros, uso indevido e roubo de informações e diversos outros problemas que possam comprometer os princípios básicos da segurança da informação,
- Aumentar a produtividade dos usuários por meio de um ambiente mais organizado e com maior controle sobre os recursos de informática e
- Viabilizar aplicações críticas das empresas.

Áreas de Atuação nos termos da IN (Instrução Normativa) 558 da CVM:

Área	Atua
Gestão de carteiras	SIM
Consultor de Valores Mobiliários	NÃO
Distribuição dos Fundos próprios	SIM
Administração Fiduciária	NÃO

Produtos:

- Produtos Estruturados.

Diretores Responsáveis:

Gestão	Pedro Zuaid Dias Soares	Riscos	Christian F. Ares Fogaccia
Distribuição	Roberto Profili	Compliance e PLD	Christian F. Ares Fogaccia
Consultoria	N/A	Suitability	Roberto Profili

III - Introdução

Informação compreende qualquer conteúdo ou dado que tenha valor para uma determinada empresa ou pessoa e que possa ser armazenado, transferido ou manipulada de algum modo, servindo a determinado propósito (e.g., tomada de decisão). Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Dentro deste contexto, toda e qualquer informação deve ser correta, precisa e estar disponível para a pessoa adequada. Portanto, Segurança da Informação[1]se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa.

De acordo com o RFC 2196 (The Site Security Handbook), uma política de segurança[2] consiste num conjunto formal de regras que devem ser seguidas pelos usuários de informações de uma organização ou de uma pessoa.

IV – Princípios Básicos da Segurança da Informação

- **Confidencialidade**: limita o acesso a informação tão somente às pessoas ou instituições autorizadas pelo proprietário da informação;

- **Integridade**: 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);

- **Disponibilidade**: garante que a informação esteja sempre disponível para o uso por aqueles usuários autorizados pelo proprietário da informação.

V – Confidencialidade

V.1 – Informações Confidenciais

São consideradas informações confidenciais para a **EuvCapital** todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível acessadas pelo colaborador em virtude do desempenho de suas atividades que possa incluir:

[1]O conceito de Segurança da Informação está padronizado pela norma ISO/IEC17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799.

[2] RFC 2196 (The Site Security Handbook)

- Know-how, técnicas, diagramas, modelos, e programas de computador;
- Informações técnicas, financeiras, mercadológicas ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela **EuvCapital**;
- Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela **EuvCapital**;
- Estruturas e planos de ação;
- Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
- Qualquer informação relativa às atividades da **EuvCapital** e a seus sócios ou clientes;
- Informações e recursos disponíveis a projetos e trabalhos críticos para a continuidade do negócio da organização; ou
- Toda e qualquer informação que por força de lei seja obrigatório o sigilo e confidencialidade.

V.2 – Informações de Uso Público

São consideradas informações de uso público todas as informações que por força de lei a **EuvCapital** é obrigada a divulgar à CVM e/ou para qualquer entidade de classe que a **EuvCapital** faça parte, desde que não conflite com o item V.1.

V.3 – Avisos Importantes em E-mails

Todos os e-mails da **EuvCapital** que possuem informações confidenciais devem conter *disclaimer* nos seguintes termos:

Esta mensagem pode conter informação confidencial e/ou privilegiada. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não pode usar, copiar ou divulgar as informações nela contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu esta mensagem por engano, por favor avise imediatamente o remetente, respondendo o e-mail e em seguida apague-o.

This message may contain confidential and/or privileged information. If you are not the addressee or authorized to receive this for the addressee, you must not use, copy, disclose or take any action based on this message or any information herein. If you have received this message in error, please advise the sender immediately by reply e-mail and delete this message.

V.4 – Avisos importantes em apresentações

Toda apresentação a clientes, contrapartes comerciais, fornecedores e prestadores de serviços que contenham informações classificadas como confidenciais deve conter:

- Aviso que o material é confidencial e de propriedade da **EuvCapital;** e
- Todas as páginas devem conter a mensagem de "informação confidencial".

V.5 – Transporte de Informações Confidenciais

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da **EuvCapital** e circulem em ambientes externos à **EuvCapital** com estes arquivos sem a devida autorização do Coordenador Sócio-Diretor responsável pela estruturação e/ou gestão do fundo.

V.6 – Segregação de Atividades

A administração de carteiras de valores mobiliários deve ser segregada das demais atividades exercidas pela pessoa jurídica ou por sua controladora, por meio da adoção dos seguintes procedimentos (IN 558, art. 24):

V.6.1. *Chinese Wall*

Com a finalidade de se evitar o uso e o acesso a informações privilegiadas, a **EuvCapital** utiliza-se do conceito *Chinese Wall*, o qual segrega as informações de Colaboradores envoltos em atividades de gestão de carteiras da área de consultoria empresarial.

Este muro de informações é controlado e mantido pelo Diretor de Compliance que tem acesso a informações de ambos os lados e se incumbe de manter a integridade da segregação, através da supervisão das atividades da Sociedade e de seus Colaboradores.

A comunicação entre as áreas separadas pelo *Chinese Wall* deve ser feita como se fossem de empresas distintas, seguindo as normas desta Política de Segurança da Informação, e a área de Compliance deve ser copiada ou chamada para as reuniões.

Os Colaboradores que exercem a atividade de gestão de carteiras devem desenvolver e manter registros apropriados para fundamentar as suas análises, recomendações, decisões de investimento e outras comunicações relacionadas aos investimentos originados pela consultoria empresarial.

V.6.2. Criação e Manutenção de Usuários

Os acessos internos e externos aos serviços de rede da **EuvCapital** são liberados de acordo com a função que o Colaborador exerce na empresa e de acordo com a sua necessidade. O Diretor da Área é o responsável por definir os acessos dos seus respectivos Colaboradores.

Todas as senhas devem ser trocadas periodicamente (no máximo 60 dias) de forma a dificultar a ação de "hackers".
Quando do desligamento de Colaboradores, o seu acesso à rede e e-mail é revogado a partir do momento que o desligamento for informado à Área de TI.

V.6.3. Proteção de Senhas

A criação de acesso dos usuários descritos no item anterior requer a criação de senha de acesso pessoal para cada usuário. Além disso, os Colaboradores não devem revelar sua senha a ninguém e nem a deixar anotada em qualquer lugar em que possa ser facilmente vista, haja visto que o mesmo é responsável por qualquer atividade a ela relacionada.

Os erros ao digitar a senha serão monitorados para se verificar a possível tentativa de invasão da rede da empresa. A responsabilidade pelo monitoramento é da área administrativa.

V.7 – Firewall

Alteração da configuração do firewall: somente a área de suporte técnico pode proceder com qualquer alteração da configuração do firewall mediante solicitação exclusiva da Diretoria da **EuvCapital**.

Monitoramento do firewall: é de responsabilidade do departamento administrativo o monitoramento do firewall da empresa.

V.7 – Segurança das Instalações

- A **EuvCapital** não faz uso de servidor físico, as informações vitais gravadas na rede são armazenadas estantaneamente na nuvem através da tecnologia Microsoft OneDrive. Em caso de inviabilidade de uso do escritório, a contingência é acionada de acordo com o Plano de Continuidade de Negócios definido.

- O acesso a única porta do escritório da **EuvCapital** é feito através da leitura digital dos Colaboradores. O uso da chave da porta somente é usado quando há queda de energia elétrica por mais de 6 horas. No caso de perda da chave do escritório, o evento deve ser comunicado imediatamente ao **Diretor de Compliance** e o mesmo deve providenciar a troca do segredo e confecção de novas chaves para os seguintes:
    - Gerente Administrativa
    - Diretor Comercial
    - Sócio Controlador

VI – Integridade

Para garantir a integridade das informações, a **EuvCapital** adota os seguintes procedimentos para reduzir o ataque de ameaças externas que possam corromper as informações arquivadas:

VI.1 – Correio Eletrônico

O e-mail da **EuvCapital** é de uso estritamente profissional, não devendo ser utilizado para fins pessoais. Os Colaboradores não poderão usar intencionalmente o e-mail da **EuvCapital** para distribuir "correntes", brincadeiras, enviar material ofensivo, inadequado, vírus ou que promova qualquer tipo de discriminação racial. Se o Colaborador receber um e-mail para distribuição a outras pessoas, como uma corrente, não poderá enviá-lo. Se tiver qualquer suspeita de que recebeu um vírus, o Colaborador deverá entrar em contato com a Área de TI imediatamente.

VI.2 – Internet

- **Uso da Internet:** estritamente profissional não devendo ser utilizado para fins pessoais. Os Colaboradores não poderão entrar em sites com conteúdo ofensivo, inadequado ou que promova qualquer tipo de discriminação racial, social ou moral.

- **Monitoramento:** a área administrativa poderá monitorar os sites que os colaboradores navegam de forma a verificar se estes estão utilizando a Internet somente para fins profissionais.

VI.3 – Instalação e Download de Softwares

Todo software somente poderá ser instalado mediante autorização prévia da Área de Administrativa.

Download de aplicativos: é proibido baixar qualquer tipo de software não autorizado pela área administrativa em função de aplicativos não autorizados poderem abrir brechas no firewall da **EuvCapital**.

VI.4 – Proteção Antivírus

- Utilização e atualização do antivírus: todo computador e servidor do **EuvCapital** deve utilizar um antivírus que possua atualização diária programada de forma automática.

- O antivírus tem que ser configurado de forma a verificar ameaças da internet, de e-mails, de sistemas de mensagem instantânea (e.g., skype) e de todo e qualquer origem de fonte de informação externa a organização.
    - É de responsabilidade dos Colaboradores a atualização do antivírus em seus computadores.
    - É de responsabilidade da área administrativa a atualização do antivírus nos servidores e de verificar se os equipamentos estão com o antivírus atualizado.

    - A renovação da licença do antivírus é realizada automaticamente.

VI.5 – Monitoramento dos Meios de Comunicação

O intermediário que atue em mercado organizado deverá manter sistema de gravação de todos os diálogos e mensagens mantidos com seus clientes, inclusive por intermédio de prepostos, de forma a registrar as ordens transmitidas por telefone ou outros sistemas de transmissão de voz.

Portanto, todas as transmissões de ordens de negociação de ativos dos fundos sob gestão da **EuvCapital** são gravadas pelos intermediários contratados pela **EuvCapital** nos termos do parágrafo acima.

Para assegurar o fiel cumprimento das regras internas, como também da legislação vigente, a EuvCapital se reserva no direito de rastrear, monitorar, gravar e inspecionar todos e qualquer tráfego de informação realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via: internet, intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), bem como os arquivos armazenados ou criados pelos recursos da informática pertencentes a EuvCapital ou utilizados em nome dela.

Todas as ligações da **EuvCapital** são gravadas e os demais meios de comunicação são monitorados e passíveis de serem auditados pelo Diretor de Compliance para verificação do cumprimento do Código de Ética e desta Política de Segurança da Informação.

VI.6 – Monitoramento da Rede

Trilhas de auditoria registrando as exceções e outros eventos de segurança relevantes:

- Produzidas e mantidas por um período de tempo determinado pela área Administrativa.
- É de responsabilidade da área administrativa monitorar as trilhas de auditoria e os acessos as pastas, arquivos e rede de forma a verificar qualquer violação das regras acima.

VI.7 – Monitoramento dos Sistemas

- Execução de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.
- Execução de auditorias e inspeções nos registros e verificação se os sistemas são protegidos contra adulterações.

VII – Disponibilidade

VII.1 – Segurança dos Processos Vitais

Entende-se por ativos vitais todos aqueles que, em caso de roubo, explosão, incêndio, quebra, perda ou mau funcionamento, podem prejudicar o andamento do processo de seleção e alocação de ativos da **EuvCapital** e trazer perdas para a mesma e/ou aos seus clientes.

Os equipamentos e serviços vitais da **EuvCapital** estão descritos no Plano de Continuidade de Negócios.

Quando ocorrer impossibilidade de acesso aos equipamentos e serviços vitais, a contingência deverá ser acionada de acordo com o Plano de Continuidade de Negócios.

A área de Compliance deve avaliar quais equipamentos vitais devem possuir seguro contra roubo, furto, incêndio e explosão. A responsabilidade pela contratação e renovação do seguro é de responsabilidade do Diretor de Financeiro.

Vide Plano de Continuidade de Negócios.

VII.2 – Manutenção de Arquivos

Todo e qualquer arquivo, documento, relatório, pesquisa, banco de dados, sistema e planilha da **EuvCapital** deverá ser salvo na rede.

A **EuvCapital** deve manter digitalmente, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos pela CVM, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções (IN 558, art. 31).

É de responsabilidade de todos os Colaboradores gravar e manter as informações da **EuvCapital** na rede.

VII.3 – Plano de Continuidade dos Negócios

O Plano de Continuidade dos Negócios consiste de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços vitais sejam devidamente identificados e preservados após a ocorrência de qualquer situação que afete os processos críticos do negócio, e até o retorno à situação normal de funcionamento da **EuvCapital**.

Vide o Plano de Continuidade de Negócio para obter mais informações a respeito.

VII.4 – Monitoramento

Para garantir a continuidade dos serviços, os recursos dos equipamentos devem ser constantemente monitorados, permitindo não só a identificação de possíveis problemas mas também, futuras atualizações de acordo com a tendência de crescimento de seus programas e aplicativos.

O monitoramento desses recursos deve verificar:

- Espaço disponível em disco,
- Processamento,
- Utilização de memória,
- Inventário de segurança,
- Conectividade,
- Estabilizadores, e
- Conectividade de rede.

VII.5 – Realização de Cópias de Segurança

- **Cópia de segurança são** feitas cópias do servidor semanalmente.

VIII – Adesão à Política de Segurança da Informação

Para garantir os princípios da segurança da informação, é preciso assegurar que cada Colaborador esteja em conformidade com as normas descritas nessa Política e nas leis que regem o setor de atuação da **EuvCapital**. Além disso, a gestão da segurança da informação necessita do apoio e participação de todos os Colaboradores.

Para tanto, são necessários os três passos a seguir:

- Treinamento e compreensão a essa política;
- Assinatura do Termo de Compromisso e Confidencialidade (Anexo I do Código de Ética); e
- Reciclagem anual.

O cumprimento desses três passos é de responsabilidade do Diretor de Risco e Compliance, o qual seguirá as seguintes regras:

- Processo de integração e treinamento inicial dos Colaboradores, aos quais, antes do início de suas atividades, será apresentada a Política de Segurança da Informação em conjunto com o Plano de Continuidade de Negócios da **EuvCapital**, bem como as principais leis e normas aplicáveis às suas atividades;
- Toda e qualquer dúvida, questionamento, sugestão ou pedido de esclarecimento relacionado a tal Política e a tal Plano, ou quaisquer outras, deverão ser respondidos em até 3 (três) dias úteis para que os Colaboradores possam compreendê-los e observá-los integralmente no desempenho das suas respectivas atividades; e

O programa anual de reciclagem dos Colaboradores tem a sua participação obrigatória, com o objetivo de fazer com que os mesmos estejam sempre atualizados em relação às regras de segurança da informação aplicáveis pela **EuvCapital**.