MANUAL DE SEGURANÇA DA INFORMAÇÃO

A Unifinance Agente Autônomo de Investimentos doravante denominada simplesmente "Unifinance" tem como único objetivo a distribuição de valores mobiliários, visando o lucro no longo prazo que advirá das taxas de administração e de performance. Nosso mais importante recurso é o capital humano, que deve se diferenciar pela sua qualidade, pela sua reputação e pelo seu preparo. A sua inserção em uma cultura de excelência e de resultados permitirá o alcance do nosso objetivo.

Para apoiar o cumprimento de seu objetivo, a Unifinance implementa e mantém uma estrutura rígida e transparente de filosofia de investimento, governança corporativa, regras de ética e conduta, controles internos e gestão de riscos.

Alguns importantes instrumentos foram desenvolvidos de forma a orientar e reger as condutas dos sócios e os colaboradores, internos e externos, doravante denominados em conjunto simplesmente "colaboradores", no processo de cumprir estes objetivos. São eles o Código de Conduta Profissional dos Agentes Autônomos de Investimento da entidade credenciadora (ANCORD), Código de Ética e Conduta da Unifinance, Programa De Treinamento e Educação Continuada, Política De Conheça Seu Cliente, Política de Antissuborno e Anticorrupção, Política De Segurança Da Informação e Segurança Cibernética, Política de Combate à Lavagem de Dinheiro, Política de Investimento Pessoais, Lista de Pessoas Expostas Politicamente, Manual de Compliance, Política de Proteção de Dados, Política de Boas Práticas, Política de Responsabilidade Socioambiental e Sustentabilidade.

Estes documentos representam o compromisso da Unifinance junto aos investidores, colaboradores e parceiros, demais participantes do mercado e órgãos reguladores, de que seus valores são pautados pela total transparência de atitudes, comportamentos e decisões. Eles também auxiliam no exercício das funções dos responsáveis pela determinação dos rumos da Empresa, trazem maior eficiência à tomada de decisões e melhoram o relacionamento com a sociedade, com os órgãos reguladores e com o governo, além de preservarem a consideração pelos interesses de todos os relacionados.

A seguir, apresentamos o Guia de Segurança da Informação da Unifinance.

1. INTRODUÇÃO

A definição e a implementação de um Guia de Segurança de Informação são passos essenciais para estabelecer normas, padrões, orientações e procedimentos de segurança da informação, assim como mecanismos de delegação e responsabilidades pelos processos de segurança da informação e controles internos, estabelecendo os fundamentos de Segurança da Informação para toda a empresa.

A Unifinance depende em grande parte da tecnologia para conduzir seu negócio, atendendo as suas necessidades operacionais, comerciais e estratégicas. Os sistemas de informação, a infraestrutura tecnológica, os arquivos de dados e as informações internas ou externas referentes a Unifinance são considerados ativos importantes da empresa.

Com a finalidade de acompanhar as boas práticas das organizações mundiais e as exigências dos órgãos reguladores e dos próprios clientes, e necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e que todos compartilhem da responsabilidade pelos processos de segurança utilizados para controlar a integridade, a disponibilidade e a confidencialidade dos ativos de informação da Unifinance.

As normas e políticas contidas neste Guia dizem respeito à segurança de todas as informações da Unifinance, acessadas, processadas, utilizadas, transportadas ou armazenadas em qualquer meio, de tecnologia ou de sistema. Vale ressaltar que todas as informações, mesmo aquelas aparentemente de menor importância, são um ativo da empresa e assim devem ser devidamente protegidas.

Este Guia se destina a todos os colaboradores da Unifinance, ou seja, para a totalidade de funcionários e sócios que participam da Empresa. O responsável por este Guia, pela sua implementação e transmissão aos colaboradores, assim como pela sua atualização e pela prática de todas as normas e políticas aqui contidas e o *Chief Operating Officer*.

2. SEGURANCA PESSOAL

As normas de segurança pessoal têm como objetivo minimizar a ocorrência de incidentes de segurança em função de deficiências no processo de conscientização dos colaboradores.

2.1. Treinamento de Segurança

Todo colaborador, ao ingressar na empresa, devera obrigatoriamente passar por treinamento relacionado à segurança das informações antes de iniciar suas atividades profissionais. O objetivo e que todo colaborador, de qualquer nível, que acesse qualquer ambiente da Unifinance ou gere, processe, utilize ou armazene as informações da Unifinance, em qualquer tecnologia, local ou meio, esteja perfeitamente informado das normas contidas neste Guia.

2.2. Responsabilidade dos Colaboradores

Todos os colaboradores devem observar e garantir a aplicação das políticas, normas e procedimentos de segurança determinados pela Unifinance. Para tanto, todos devem assinar o Termo de Responsabilidade, no qual assumem tal responsabilidade, quando ingressarem ou iniciarem suas atividades na empresa. Todos são responsáveis individualmente pelos equipamentos de tecnologia que

utilizam ou gerenciam. Tal compromisso será formalizado através da assinatura do referido Termo de Responsabilidade,

Nenhum colaborador deve revelar a terceiros quaisquer informações referentes aos demais colaboradores, tais como, endereço, telefone, dentre outras. Da mesma forma, nenhum colaborador deve revelar a terceiros quaisquer informações referentes a clientes, tais como, identidade, informações pessoais, investimentos, dentre outras.

Incidentes e dúvidas sobre assuntos relacionados à segurança da informação devem ser reportados imediatamente e não devem ser divulgados a terceiros ou outras partes que não estejam diretamente envolvidas com o incidente.

Se houver perda ou roubo de algum equipamento, o *Chief Operating Officer* deve ser informado imediatamente para bloqueio remoto do mesmo. Todas as informações quando impressas devem ser acompanhadas e retiradas imediatamente das impressoras. Arquivos não podem ser duplicados na rede. A fonte deve ser única para mitigar a possibilidade de perdas de informações por arquivos duplos.

2.3. Circulação de Informações

Todas as informações da Unifinance são consideradas críticas para o negócio e devem ser consideradas como confidenciais, salvo disposição em contrário. Nenhuma informação crítica ou confidencial da Unifinance pode ou deve ser discutida em locais inapropriados como locais públicos ou locais fechados com a presença de terceiros ou pessoas não diretamente relacionadas com o assunto ou sem autorização de acesso e conhecimento dessa informação.

Todos os colaboradores estão proibidos de fazer transitar por qualquer meio externo as dependências da Unifinance, quaisquer informações que não sejam de domínio público, sem consentimento do Comitê Executivo. Desta forma, todo o trabalho deve ser prioritariamente realizado nas dependências da empresa. O uso de discos removíveis e proibido, mas casos excepcionais podem ser previamente analisados e aprovados pelo Comitê Executivo.

A rede interna não pode ser utilizada para a conexão de notebooks pessoais ou outros equipamentos, salvo se autorizado pelo Comitê Executivo. Todas as ligações feitas por telefone fixo serão gravadas e armazenadas pelo prazo de 5 (cinco) anos, a contar da data da realização das ligações.

3. SEGURANÇA FÍSICA

As normas têm como objetivo proteger os recursos de tecnologia da Unifinance contra fatores que possam causar a interrupção das atividades, a alteração das informações ou prejuízos financeiros.

3.1. Proteção dos Equipamentos

Todos os equipamentos considerados críticos para as atividades da Unifinance, servidores, por exemplo, devem ser mantidos em local seguro, cujo acesso seja controlado e restrito. Este local deve estar preferencialmente protegido contra desastres físicos.

O acesso a este local deve ser concedido pelo *Chief Operating Officer*, de acordo com as necessidades dos colaboradores ou prestadores de serviço para execução de suas tarefas e pelo prazo necessário. O acesso de terceiros ao local onde são mantidos os equipamentos críticos deve ser registrado e estar acompanhado permanentemente por um colaborador autorizado pelo *Chief Operating Officer*. Os terceiros devem estar devidamente identificados, por meio da utilização de crachás, quando estiverem em tais dependências.

Todos os colaboradores são responsáveis individualmente pelos equipamentos de tecnologia que utilizam ou gerenciam. Deve existir um comprometimento formal pelo uso adequado e cuidadoso com os equipamentos de tecnologia utilizados. Não é permitido o consumo de comidas ou bebidas nos locais onde estão armazenados os equipamentos críticos, bem como o uso de cigarros ou outros fatores geradores de qualquer tipo de resíduo solido ou gasoso que não os de proteção da operação.

3.2. Equipamentos de Tecnologia

A Unifinance deve possuir recursos que possibilitem a continuidade das operações no caso de interrupções no fornecimento de energia. A Unifinance deve possuir sistemas e recursos de contingência remota que possibilitem a continuidade das operações mesmo na impossibilidade de se fazer uso das instalações principais da empresa.

Todo o cabeamento de rede e energia deve ser feito, sempre que possível, de forma embutida ou por meio da utilização de conduítes. Preferencialmente, o cabeamento da rede deve ser segregado do cabeamento de energia.

Somente o *Chief Operating Officer*, ou alguém por ele autorizado, poderá instalar, desinstalar e dar manutenção nos equipamentos da Unifinance. Toda a manutenção deve seguir as recomendações do fabricante do produto.

Todo equipamento removido das dependências da Unifinance para uso ou manutenção externa deve ser autorizado pelo *Chief Operating Officer* e registrado para controle e acompanhamento. Qualquer conteúdo de equipamentos ou mídias que venham a ser descartados deve ser preliminarmente eliminado. Se isto não for possível, o equipamento ou a mídia deve ser destruído fisicamente.

As mídias que contêm informações críticas devem ser desmagnetizadas quando forem ser reutilizadas; na impossibilidade desta ação elas devem ser destruídas.

3.3. Controle Geral do Ambiente

Todas as mídias utilizadas para armazenamento de dados devem ser identificadas quanto ao conteúdo e a data de criação. Toda mídia deve ser armazenada adequadamente quando não estiver em uso, de forma que sua confidencialidade, integridade e disponibilidade não sejam comprometidas.

Todos os equipamentos devem ser protegidos por senha quando não estiverem sendo utilizados. E responsabilidade do usuário assegurar este requisito. Todas as senhas devem ser individuais e mantidas confidenciais pelos seus proprietários e não devem ficar expostas para consulta nem serem anotadas em papel ou em qualquer outro local. Os usuários são responsáveis por todas as atividades realizadas com seus *logins* e senhas. Não devem ser utilizadas senhas de fácil adivinhação como, por exemplo, data de aniversário, nome, sobrenome, dentre outras.

3.4. Dependências da Unifinance

É vedado o acesso de visitantes as dependências da Unifinance sem acompanhamento de um colaborador responsável pela visita. Estão incluídos como visitantes os prestadores de serviços, funcionários de empresas de auditoria ou órgãos reguladores e prestadores de serviço de manutenção de software. Os colaboradores não devem divulgar aos visitantes, em qualquer hipótese, sua senha de acesso ao computador.

É vedado o acesso de visitantes as mesas de trabalho, salvo se na presença de um colaborador responsável, que anteriormente se assegurou de que não há informações (principalmente nomes de clientes) expostas. Os trabalhos com terceiros deverão ser desenvolvidos em salas de reuniões, sendo que a permanência do visitante nestas está condicionada a permanência do colaborador responsável pela visita na empresa.

4. COMUNICAÇÃO E GERENCIAMENTO DA INFORMAÇÃO

4.1. Proteção contra Vírus e Software não Autorizado

Todos os arquivos armazenados na rede e e-mails devem ser protegidos por software antivírus, que deve estar sempre atualizado e ativo.

As mídias recebidas do meio externo devem ser verificadas quando a existência de vírus antes de serem atualizadas. É terminantemente proibida a instalação de qualquer software sem licença de uso ou executada por pessoas que não sejam autorizadas.

Não é permitido o download de softwares da internet, salvo com autorização do *Chief Operating Officer*. A instalação de qualquer software somente poderá ser feita com autorização do *Chief Operating Officer.*

4.2. Cópias de Segurança – Backup

Todas as informações utilizadas na operação da Unifinance devem possuir cópia de segurança. A periodicidade com a qual serão realizadas tais cópias será definida de acordo com a criticidade da informação ou do sistema.

Devem ser realizados testes regulares com as mídias de backup para assegurar que as informações poderão ser restauradas, se necessário. O procedimento para restauração das mídias de backup deve ser solicitado ao *Chief Operating Officer*, autorizado pelo proprietário da informação e formalmente documentado.

As mídias de backup devem ser armazenadas de forma segura, de preferência em lugar distante das instalações físicas onde são processadas. O período de retenção das mídias de backup dependerá do tipo de informação que está armazenada ou da existência de alguma legislação específica.

4.3. Transmissão de Informações

Somente informações de domínio público podem ser transmitidas em qualquer meio de comunicação. Todas as informações - que trafegam fora do ambiente fisicamente seguro da Unifinance - devem estar preferencialmente criptografadas.

Todas as mensagens enviadas via correio eletrônico (e-mail) são consideradas como comunicação formal da Unifinance. Desta forma, seu conteúdo deve ser ponderado antes de sua emissão e seu conteúdo poderá ser acessado pelo Comitê Executivo a qualquer momento.

O uso do correio eletrônico (e-mail) deve ser destinado somente para as atividades relacionadas ao negócio da Unifinance. Atividades como envio de correntes, engajamento em qualquer atividade ilegal, imprópria ou não ética não são permitidas, assim como o uso de linguagem ou imagens impróprias, obscenas ou de baixo calão.

4.4. Uso da Internet

O acesso à internet deve ser realizado para finalidades relacionadas aos interesses e assuntos profissionais da Unifinance. Todos os acessos realizados a internet são monitorados. O acesso a sites de conteúdo inapropriado, tais como pornografia ou atividades criminais não é permitido.

Todos os acessos à internet devem ser feitos por meio da rede interna da Unifinance, passando obrigatoriamente pelo firewall. Todos os usuários devem possuir login e senhas únicas para acesso à internet, que devem expirar e ser renovados periodicamente.

4.5. Controle de Acesso

É um objetivo da Unifinance que pessoas não autorizadas não obtenham acesso ao ambiente de tecnologia e, consequentemente, as informações da empresa, assegurando a integridade, a confidencialidade e a disponibilidade das informações que a Unifinance utiliza em suas operações.

Os acessos a determinados tipos de informação ou sistema somente poderão ser concedidos pelos proprietários da informação. A concessão do acesso somente poderá ser efetuada de acordo com as necessidades do colaborador ou prestador de serviço para execução de suas atividades.

Não devem ser utilizados usuários genéricos para concessão de acesso a um determinado ativo de informação ou sistema. Todos os colaboradores e prestadores de serviço da Unifinance deverão ser identificados por um login e senha únicos. Será terminantemente proibida a utilização de logins e senhas de outros colaboradores em qualquer situação.

Qualquer transferência, férias ou desligamento de colaboradores, assim como encerramento de contrato com terceiros, deve ser comunicado imediatamente para que seja providenciado o bloqueio e remoção do login e dos acessos de tais usuários.

A rede interna da Unifinance poderá ser acessada somente pelos seus colaboradores e outros colaboradores devidamente autorizados e justificados, mediante a autenticação do login e da senha do usuário.

Deve existir um padrão de configuração para acesso remoto de usuários, com restrições determinadas por suas atividades e devidamente controladas.

5. VIOLAÇÕES E PENALIDADES

São consideradas violações à Política de Segurança da Informação as seguintes situações, não se limitando as mesmas:

- Quaisquer ações ou situações que possam expor a Unifinance a perda financeira ou de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

- Uso indevido de dados corporativos, divulgação não autorizada de informações ou de segredos comerciais ou outras informações sem a permissão expressa do proprietário;

- Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da Unifinance;

- A não comunicação imediata ao órgão competente pela segurança da informação de quaisquer violações ou atitudes anormais de que porventura um colaborador venha a tomar conhecimento ou chegue a presenciar; e

- O não cumprimento de qualquer norma desta Política de Segurança da Informação.

A violação das normas deste Guia e considerada falta grave, podendo ser aplicadas penalidades de acordo com a sugestão do *Chief Operating Officer*, a ser aprovada pelo Comitê Executivo, como segue:

- Advertência;

- Aplicação de ações disciplinares;

- Término ou cessão do contrato de prestação de serviço ou relação comercial; e

- Processo civil ou criminal.