Áfira
INVESTIMENTOS

Março 2021

Manual de Segurança da TI

Este Manual deverá ser atualizado, no mínimo anualmente, ou quando da alteração de procedimentos imposta por normas internas e/ou externas.

CONTEÚDO

1. INTRODUÇÃO

O Manual de Segurança da TI da Áfira Investimentos ("Áfira" ou "Gestora") tem por objetivo nortear o adequado gerenciamento das informações de posse temporária ou de propriedade da Gestora. Assim, deverá ser seguida por todos os seus Colaboradores.

Este Manual foi elaborado em estrita observância às normas aplicáveis às atividades desempenhadas pela Áfira e tem propósito de definir o Plano de Continuidade de Negócios ("PCN") para os eventos que impliquem em impossibilidade na operação normal do escritório principal da Áfira, incluindo as atribuições e responsabilidades dos Colaboradores na execução do plano.

2. CONCEITOS

2.1 CONFIDENCIALIDADE

Os Colaboradores deverão observar as regras de confidencialidade previstas no 'Manual de Ética e Conduta' disponibilizado no site da empresa (www.afirainvestimentos.com).

Qualquer informação sobre a Áfira, suas atividades, seus sócios e clientes só poderá ser compartilhada com terceiros com a autorização formal do Diretor de Risco e Compliance.

2.2 CONTROLES DE ACESSO A INFORMAÇÕES CONFIDENCIAIS

Todos os acessos a informações são segregados em diretórios com chaves individuais de acesso para quem de direito na função.

O controle do acesso a sistemas de informações da Gestora considera que:

a) Compatibilidade de nível de acesso ao seu perfil; e
b) Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora.

2.3 TRATAMENTO

Todas as Informações Sigilosas constituem ativos de valor para a Sociedade, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Sociedade, Clientes, Fundos, Carteiras e Colaboradores.

As Informações Sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Sigilosas deve ser prioridade constante da Sociedade, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da Sociedade.

Assim, por princípio, a guarda e segurança das Informações Sigilosas deve abranger três aspectos básicos, destacados a seguir:

(i) Acesso: Somente pessoas devidamente autorizadas pela Sociedade devem ter acesso às Informações Sigilosas;

(ii) Integridade: Somente alterações, supressões e adições autorizadas pela Sociedade devem ser realizadas às Informações Sigilosas; e

(iii) Disponibilidade: As Informações Sigilosas devem estar disponíveis para os Colaboradores autorizados sempre que necessário ou for demandado.

Para assegurar os 3 (três) aspectos acima, as Informações Sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

3. RESPONSABILIDADES

3.1 Comitê de Risco e Compliance

Para fim da prática do Plano referido, o Comitê de Risco e Compliance deve:

a) Definir o conteúdo do PCN;
b) Comunicar a todas as áreas afetadas quanto à obrigatoriedade de aplicação do PCN;
c) Tomar as ações necessárias em caso de evento que implique na necessidade de colocação do PCN em operação.
d) Garantir que o PCN esteja em concordância com as leis e normas dos órgãos reguladores;
e) Garantir que o PCN esteja permanentemente atualizado e que o Diretor de Risco cumpra o cronograma de treinamento nele previsto.

3.2 Diretor de Risco

O Diretor de Risco deve:

a) Garantir que o PCN esteja sempre pronto para ser colocado em operação, realizando as rotinas diárias de replicação de bases de dados e sistemas;
b) Revisar e ajustar o PCN sempre que mudanças nas rotinas operacionais assim justificarem;
c) Organizar e realizar treinamentos periódicos de ativação simulada do PCN, no mínimo anualmente, emitindo relatório de ocorrências com sugestão de medidas corretivas para o Comitê de Risco e Compliance.

3.3 Colaboradores

Todos os Colaboradores devem respeitar e garantir o cumprimento do PCN.

4. PLANO DE CONTINUIDADE DE NEGÓCIOS

O PCN da Áfira é um plano logístico de implementação prática especificando de que forma funções críticas da operação normal serão total ou parcialmente restabelecidas, dentro de um tempo máximo pré-determinado, em uma situação de desastre ou interrupção forçada das operações.

4.1 Princípios Gerais

Os princípios gerais que norteiam o PCN são:

a) Criticidade. O restabelecimento de funções críticas terá precedência sobre quaisquer outras enquanto perdurar a situação anormal. São consideradas críticas as funções que garantam a preservação do patrimônio líquido sob gestão da Áfira;
b) Prontidão. O PCN deve ser acionado imediatamente após a ocorrência da situação de desastre ou interrupção forçada das operações, de modo a minimizar o tempo de restabelecimento das funções críticas;
c) Priorização. A execução do PCN até a completa normalização das operações deverá ter prioridade absoluta sobre quaisquer outros projetos em andamento.

4.2 Virtualização e Backup de Sistemas

A Áfira possui um sistema crítico rodando em suas instalações. O Virtual software é o sistema contratado para gestão das carteiras e emissão de relatórios dos clientes com sobreposição de um sistema proprietário da Áfira.

As informações estão depositadas em uma base Microsoft-SQL, com rotina diária de backup em servidor duplicado, tendo backup no endereço da gestora além do alocado na AWS.

Todos os arquivos e dados importantes são automática e continuamente replicados em servidor externo, podendo ser acessados remotamente em caso de contingência.

4.3 Telefonia

Temos contratado o serviço da L5 Networks Comercio em Telecomunicações e Informática LTDA, CNPJ 04.281.252/0001-50, com sede na Rua André Ampére, 153 – 16º andar - Brooklin Novo, São Paulo, SP, Brasil. Dentre os serviços disponíveis no PCN, estão:

a) Gravação automática das conversas telefônicas;
b) Ramais físicos (telefones IP) com contingência via celular;
c) Central PBX Virtual completa;
d) Configuração centralizada 100% via web;
e) Sistema espelhado em 8 datacenters (1 no Brasil, 1 no México e 6 nos EUA);
f) Sistema via internet.
g) Religamento imediato do sistema, alterando a fonte de dados;

4.4 Local físico de contingência

O sistema pode ser acessado a qualquer momento remotamente. No caso de materialização de uma contingência, os colaboradores poderão ser autorizados a trabalhar de qualquer local por intermédio de internet, utilizando equipamento autorizado pela área responsável.

4.5 Procedimentos

Na ocorrência de evento que implique em ativação do PCN, o Diretor de Risco instruirá aos Colaboradores que deverão seguir os procedimentos anteriormente estabelecidos e divulgados.

5. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

5.1 Adoção de Comportamento Seguro

Independente do meio e/ou forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da Sociedade e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

a) Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;

b) Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das Informações Sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;

c) Todo tipo de acesso aos dados e informações da Sociedade, em especial as Informações Sigilosas, que não for expressamente autorizado é proibido;

d) Assuntos relacionados ao desempenho de atividades e funções na Sociedade não devem ser discutidos em ambientes públicos ou em áreas expostas (e.g. meios de transporte, locais públicos, encontros sociais);

e) As senhas de acesso do Colaborador aos sistemas da Sociedade são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;

f) Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;

f) Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter Informações Sigilosas. Portanto, não podem ser parcial ou totalmente divulgadas, usadas ou reproduzidas sem o consentimento prévio do remetente ou do autor. Toda e qualquer divulgação, uso e/ou reprodução não expressamente autorizada é proibida;

g) Documentos impressos e arquivos contendo Informações Sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da Sociedade sem a autorização prévia do superior hierárquico do Colaborador; e

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Sociedade. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento à terceiros, bem como com conteúdo político ou outro que possa colocar a Sociedade em risco.

5.2 Gestão de Acesso

A Áfira disponibiliza mecanismos de segurança visando à proteção da informação, segregados em:

(a) senhas de acesso à rede: todas as Pessoas Vinculadas que exercem sua atividade dentro do ambiente de trabalho da Áfira serão portadores de senhas individuais e intransferíveis de acesso, conforme procedimentos apresentados pelo Departamento de Compliance. Nas hipóteses de desligamento de Pessoas Vinculadas, o superior imediato será o responsável por desativar o acesso, com imediata comunicação ao Departamento de Compliance;

(b) arquivamento de documentos: os documentos físicos rotulados como de acesso restrito e de caráter sigiloso serão guardados em local fechado e com acesso limitado a pessoal autorizado. O processo de controle de depósito e retirada de documentos é restrito a pessoas devidamente autorizadas e a disponibilidade dos documentos é garantida por processo criterioso desde o momento do arquivamento.

(d) controle e guarda de documentos eletrônicos: a Áfira se esforça para digitalizar os documentos e arquivos que se encontrem em sua posse, de modo a facilitar o acesso a eles por Pessoas Vinculadas autorizadas e, de igual forma, seu arquivamento. O arquivamento é feito de forma eletrônica e em pastas com perfis pré-determinados de acesso, de modo a restringir o acesso a estes documentos apenas àqueles que deles necessitem para que suas funções sejam devidamente exercidas;

5.3 Registro e controle de acesso

O controle de segurança centralizado em módulo específico utiliza diversos níveis de segurança, tanto no acesso ao sistema e aos menus, quanto na visualização e controle de acesso. Todo acesso é passível de rastreamento pelo sistema.

- Registra todas as operações executadas em tabela ou arquivo de log;
- Toda operação é identificada por data, hora, identificação do usuário;
- Possui opção para criação e manutenção do cadastro de usuários;
- Controla a validade, suspensão e expiração dos usuários;
- Permite imprimir relatório de usuários e níveis de acesso;
- Grava as senhas dos usuários e o armazenamento é criptografado;
- Controla a validade da senha inibindo acesso por expiração de prazo;
- Permite definir de forma parametrizada a estrutura de senhas (quantidade de caracteres, alfa, numérico, caracteres especiais, etc.);
- A estrutura de gestão de acessos é por usuário.
- As funções do sistema dentro do módulo de segurança são agrupadas por menu de forma a facilitar a identificação dessas no momento de atribuir os acessos aos usuários;
- Permite estabelecer níveis de acesso por módulos e funções;
- Mantém registro dos acessos aos módulos de forma a permitir consulta;
- Mantém registro das tentativas de acesso por usuários não habilitados; e
- Permite estabelecer de forma parametrizada os prazos de expiração das senhas de acesso aos usuários.

6. CONSIDERAÇÕES FINAIS

Os procedimentos aqui definidos serão testados com periodicidade mínima anual, a fim de averiguar sua efetividade em situações de interrupção forçada de operações.

Caso sejam identificadas falhas na implementação do PCN quando da realização do teste, os procedimentos aqui estabelecidos deverão ser revistos e novamente testados até que se obtenha resultado satisfatório.

+55 (21) 3579-5859
R.Visconde de Pirajá, 414-1205
Ipanema |Rio de Janeiro |Brasil
www.afirainvestimentos.com