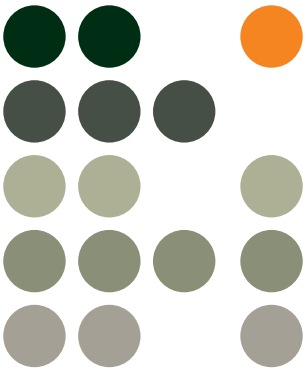

BRAINVEST

WEALTH MANAGEMENT

POLÍTICA DE **SEGURANÇA**

ÍNDICE

1 POLÍTICA DE SEGURANÇA

Autor: Brainvest Consultoria Financeira Ltda.
Data de Criação: 09 de Abril de 2012
Última Atualização: 08 de Junho de 2015
Documento: Procedimentos Internos
Versão: 1.1

2 CONTROLE DE DOCUMENTO

Autor: Brainvest Consultoria Financeira Ltda.
Data de Criação: 08 de Junho de 2015
Referência das Alterações: Não há documentos prévios
Versão: 1.1

3 ESPECIFICAÇÃO

3.1. Objetivo

Art. 1º - Estabelecer regras para a disponibilização e utilização de serviços de rede de dados, internet, telecomunicações e correio eletrônico institucional.

Art. 2º - Aprovar as políticas, normas e procedimentos de segurança da informação;

Art. 3º - Designar, defenir ou alterar as responsabilidades da área de Segurança da informação;

Art. 4º - Aprovar novos controles ou alterar as responsabilidades da área de Segurança da Informação;

Art. 5º - Apoiar a implantação de soluções para minimização dos riscos;

Art 6º - Dar suporte as iniciativas na área de Segurança da Informação;

Art. 7º - Priorizar soluções, programas e serviços baseados em software livre que promovam a otimização de recursos e investimentos em tecnologia da informação.

3.2. Responsabilidade e Proibições

Art. 8º - O monitoramento do uso da internet é importante para que sejam registrados todos os acessos de cada usuário e para que possam ser notificados e até mesmo punidos nos casos de acesso que sejam contrários a política da Brainvest.

Art. 9º - São responsabilidades dos usuários de serviços de rede de dados, internet, telecomunicações e correio eletrônico e recursos computacionais da Brainvest Consultoria Financeira Ltda:

Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como suas respectivas senhas;

Efetuar cópias de segurança de seus arquivos, catálogos de endereço, e-mails e quaisquer outros materiais de ordem digital;

Utilizar de forma ética e legal os recursos computacionais, de rede de dados, internet, telecomunicações e correio eletrônico;

Não alterar configurações dos softwares de segurança como antivírus e firewall.

Art. 10º – São proibições aos usuários de serviços de rede de dados, internet, telecomunicações e correio eletrônico e recursos computacionais da Brainvest Consultoria Financeira Ltda:

Utilizar, em quaisquer circunstâncias, os recursos da Brainvest Consultoria Financeira para difamar, prejudicar, subtrair, caluniar ou molestar outras pessoas ou empresas;

Utilizar, examinar, copiar, armanezar, distribuir ou instalar programas ou qualquer material protegido por direito autoral (copyright);

Efetuar qualquer tipo de acesso e/ou alteração em dados não autorizados;

Violar ou tentar violar sistemas de segurança da Brainvest Consultoria Financeira ou de qualquer outra empresa ou pessoa;

Fazer-se passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos da empresa;

Transmitir, difundir ou disponibilizar a terceiros, informações, dados, conteúdos, mensagens, gráficos, arquivos e som e/ou imagem, gravações, software ou qualquer classe material que, de qualquer forma, induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentos ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à orgem publica.

3.3. Senhas

Art. 11º - As senhas de acesso não devem ser compartilhadas ou divulgadas, evitando-se, assim, que outros usuários não permitidos tenham acesso a informações confidenciais ou que não lhes digam respeito.

Art. 12º - Por serem de fácil dedução, alguns critérios devem ser evitados na criação de uma senha:

números sequenciais;
datas de nascimento;
sobrenome;
placas de carros, entre outros.

Art 13º - Os sistemas devem ser configurados de forma a não permitir a criação de senha consideradas de fácil descobrimento, contendo parâmetros básicos como:

Número de caracteres para composição da senha: no mínimo seis caracteres;

Expiração de senha: deve ser forçada a alteração das senhas dos usuários no período de 6 meses;

Repetição de senhas: restringir, pelo menos, a utilização das ultimas cinco

senhas utilizadas;

Quantidado de tentativas inválidas de acesso: deve haver um limite de três tentativas para realizar o bloqueio de acesso inválido, de forma a evitar a descoberta das senhas;

Bloqueio automático por tempo de inatividade (Time out): Os sistemas devem possuir tempo máximo determinado para realizar bloqueio/término de um acesso por inatividade.

3.4. Realizações de Backups

Art. 14º - Deverão ser adotados, independentemente de seu tamanho, procedimentos de cópias de segurança (backup) e recuperação (restore) de informações.

Art. 15º - Para a implementação da cópia de segurança deve-se levar em consideração a importância da informação, o nível de classificação utilizado, sua periodicidade de atualização e também sua volatilidade, conforme as seguintes premissas:

Realizar backup visando diminuir os riscos de continuidade;
Manter os backups em local físico distante da localidade de armazenamento dos dados originais;
Verificar a integridade da informação armazenada;
Avaliar a funcionalidade dos procedimentos;
Identificar procedimentos desatualizados ou ineficazes;
Identificar falhas ou defeitos.

4 DESCUMPRIMENTO DAS REGRAS E PENALIDADES

Art. 16º - O descumprimento ou inobservância de quaiquer regras ou políticas definidas neste documento implementado pela Brainvest Weath Management são consideradas faltas graves, podendo, resultar contra o infrator, ações extrajudiciais cíveis e criminais, além de suspensão imediata de acesso e uso dos recursos

computacionais da empresa.

Art. 17º - Este Regulamento entra em vigor na data de sua criação.