MACRO INVEST

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO DA POLÍTICA

Esta política tem como objetivo estabelecer diretrizes, normas e procedimentos que visem proteger das informações de propriedade da MacroInvest e/ou sob sua guarda, preservando a confidencialidade, integridade e disponibilidade de suas informações e documentos.

A Política da Segurança da Informação deve ser seguida por todos os colaboradores da MacroInvest, devendo ser definidas e atribuídas responsabilidades no conteúdo desta Política.

A MacroInvest como gestora de recursos de terceiros, recebe, armazena e gerencia informações sigilosas de clientes e deve estar sempre atenta para a manutenção da confidencialidade das mesmas.

A informação pode ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e vídeo, etc.

Sendo assim, a segurança da informação deve abranger três aspectos:

i) Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.

ii) Disponibilidade: a informação deve estar disponível somente para as pessoas autorizadas, e sempre que necessário ou demandado.

iii) Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.

A MacroInvest possui uma Política sobre “Informações Privilegiadas”, em seu Manual de Compliance, que faz parte do arcabouço de proteção da segurança das informações.

O sucesso desta Política depende da combinação de vários elementos, dentre eles, a estrutura organizacional da empresa, as normas e procedimentos relacionados à segurança da informação e a maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, assim como o comportamento dos colaboradores.

2. ESTRUTURA E ATRIBUIÇÃO DE RESPONSABILIDADES

A MacroInvest criou um Comitê Estratégico que tem como um de seus objetivos aprovar a Política de Segurança da Informação e tomar as decisões administrativas referentes aos casos de descumprimento desta Política.

Caberá a todos os colaboradores cumprirem fielmente a Política e os procedimentos, buscando sempre orientação com seu superior hierárquico imediato em caso de dúvidas quanto segurança da Informação. Devem proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizadas pela empresa e ainda, assegurar que os recursos tecnológicos sejam utilizados apenas para as finalidades aprovadas pela empresa.

O responsável por TI deverá propor iniciativas relacionados ao aperfeiçoamento da segurança da informação, estabelecendo procedimentos de gestão dos sistemas de controle de acesso aos usuários e realizando testes e averiguações em sistemas e equipamentos com intuito de verificar o cumprimento da Política.

O proprietário da informação deverá autorizar a liberação de acesso à informação sob sua responsabilidade, mantendo o controle das liberações concedidas e cancelando aquelas que não foram mais necessárias.

3. PROCEDIMENTOS DE CONTROLE DE ACESSO

O acesso ao ambiente de rede de MacroInvest deve ser controlado de forma a garantir o acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação.

A rede deve ser acessada apenas por desktops inventariados e autorizados pela MacroInvest.

Serão utilizados identificadores de usuários (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações. O Comitê Estratégico aprovará a concessão de autorização de acesso e verificará se o nível de acesso concedido é apropriado ao propósito do negócio.

Deve ser removido o acesso a usuário desligado da empresa imediatamente, e também aqueles que tenham mudado de função.

As senhas de acesso de usuário devem ser alteradas de três em três meses. A senha é pessoal e intransferível, sendo proibido o repasse de senha para utilização por outro colaborador ou terceiros. A responsabilidade de manutenção de sua própria senha é integral do usuário.

As senhas de acesso não devem ser anotadas em arquivos físicos ou de fácil acesso. Cabe aos colaboradores memorizar as suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, números telefônicos, etc.

Por procedimentos de segurança o usuário que proceder cinco tentativas seguidas de acesso com senha inválida tem a conta bloqueada. O desbloqueio deverá ser feito com autorização de TI e de seu superior imediato.

Todas as senhas são mantidas de forma eletrônica criptografada nos bancos de dados da empresa. Algumas contas possuem diferenciações quanto ao escopo de atuação do solicitante, que definirá quais funcionalidades serão disponibilizadas para a conta criada.

4. PROCEDIMENTOS DE UTILIZAÇÃO DA REDE

As normas de utilização da rede englobam, dentre outros assuntos, a disponibilização e instalação de programas, controles de acesso ao ambiente de rede, configuração da rede e organização de diretórios. Todos os procedimentos são executados pelo TI.

Para garantir a segurança das informações da rede, algumas condutas são proibidas, tais como:

a) Realizar tentativas de acesso não autorizado, fraudando autenticação de senhas ou usuários;
b) Armazenar ou gravar arquivos de áudio ou vídeo que violem as leis de propriedade intelectual ou direito autoral, e matérias de natureza pornográfica, que atentem contra a ética e a moral dentro do ambiente de trabalho;
c) Criar arquivos que venham comprometer o desempenho e funcionamento dos sistemas;
d) Provocar congestionamentos na rede interferindo nos serviços dos usuários;
e) Instalar ou remover softwares sem o acompanhamento de IT

f) Repassar arquivos sigilosos e confidenciais da empresa a terceiros sem a autorização da diretoria da empresa. É de responsabilidade do usuário a confidencialidade dos dados gravados em pen-drive ou CD-ROM.

5. ANTIVÍRUS

Todas as estações conectadas à rede são dotadas de sistemas antivírus atualizadas automaticamente. O controle e acompanhamento das atualizações são realizados pelo IT, que identifica, isola e elimina quaisquer riscos à integridade da rede. É vedada a instalação de qualquer outro sistema de antivírus isoladamente.

6. CORREIO ELETRÔNICO - EMAIL

A utilização de e-mail é o principal veículo de comunicação na empresa, no entanto, deve ser usado de forma cautelosa, profissional e com linguagem apropriada. A empresa se reserva o direito de rastrear, monitorar e gravar quaisquer informações transmitidas via correio eletrônico.

É proibida a utilização do domínio @macroinvestgestao.com.br por terceiros que não sejam colaboradores da MacroInvest.

É proibido:

a) enviar quantidade de mensagens excessivas em um lote: spam ou junk mail;

b) enviar mensagens com excessivo tamanho de arquivos;

c) reenviar pirâmides, correntes;

d) cadastrar-se em sites de compras e entretenimentos o e-mail corporativo como contato.

7. MONITORAMENTO E CONTROLE

As informações, sistemas e os serviços utilizados pelos usuários são de exclusiva propriedade da MacroInvest, não podendo ser interpretados como de uso pessoal.

Todos os colaboradores devem ter ciência de que o uso das informações e dos sistemas podem ser monitorados e que os registros poderão ser utilizados para detecção de violações à Política

8. VIOLAÇÕES À POLÍTICA

Nos casos em que houver violação à Política e/ou procedimentos relativos à segurança da informação sanções administrativas / legais poderão ser aplicadas, podendo culminar com o desligamento do colaborador da empresa.