FINAXIS

POLÍTICA

Segurança da Informação

Maio/2019

SUMÁRIO

1. OBJETIVO

O objetivo desta política é promover melhores práticas, padrões e diretrizes para o ambiente Finaxis e seus prestadores de serviços no trato de seus ativos de informação, disseminando uma cultura de segurança das informações entre seus colaboradores, mantendo a segurança dos sistemas, a integridade e disponibilidade de dados, a confidencialidade das informações, a continuidade dos negócios e a aderência às leis e normas que regulamentam os negócios financeiros, mitigando riscos que possam resultar em perda ou prejuízo, seja de ordem financeira ou de imagem para as empresas Finaxis.

Na busca constante pela excelência de nossos serviços, esta Política é uma declaração formal das empresas que compõem o Finaxis, do seu comprometimento em proteger todos os seus ativos, apoiando metas e princípios da Segurança da Informação estabelecidos neste documento, a fim de garantir a confidencialidade, disponibilidade, integridade e legalidade das informações, alinhadas com suas estratégias de negócio.

Esta política e os demais procedimentos que suportam sua implementação estão em conformidade com as demais políticas do Finaxis.

2. PÚBLICO ALVO

A presente Política é aplicável a todos os colaboradores do Finaxis, composto pelas empresas Holding Finaxis S.A., Banco Finaxis S.A., Finaxis Corretora de Títulos e Valores Mobiliários S.A.

Aplica-se ainda, a todos os fornecedores, terceiros, prestadores de serviços e empresas que se relacionam com o Finaxis.

3. DIRETRIZES

3.1. Ativos

Todos os recursos tecnológicos disponibilizados pelas empresas do Finaxis, como computadores, e-mail, telefones, redes, acesso à Internet e sistemas se destinam única e exclusivamente aos interesses de negócio do Finaxis, no qual todos os funcionários são responsáveis pelo correto manuseio devendo zelar e proteger com a finalidade de gerar benefícios à organização e, como consequência, auxiliar no cumprimento de sua missão.

As informações acessadas, geradas ou desenvolvidas nas dependências internas ou externas da instituição por funcionários ou parceiros de negócios são consideradas ativos intangíveis devendo ser devidamente manuseadas, protegidas e utilizadas unicamente para a finalidade previamente autorizada, independente da forma como foi armazenada ou compartilhada.

A informação pode estar disponível de diversas formas: sistemas de informação, meios magnéticos, filmes, mídia impressa ou ótica, equipamentos portáteis, dispositivos eletrônicos, hardware, software ou mesmo na comunicação verbal.

3.2. Princípios de Segurança da Informação

Confidencialidade: Garante que as informações tratadas são de conhecimento exclusivo de pessoas autorizadas a acessá-las.

Integridade: Garante que as informações são mantidas íntegras, sem modificações indevidas, sejam acidentais ou propositais.

Disponibilidade: Garante que as informações estão disponíveis a todas as pessoas autorizadas a tratá-las.

Quando algum dos princípios acima não é respeitado a empresa está exposta a riscos que podem comprometer a continuidade dos negócios e afetar sua imagem perante seus clientes, parceiros e acionistas.

3.3. Acesso Físico

O acesso às dependências da empresa somente é permitido às pessoas previamente autorizadas portando crachá de identificação que deverá estar visível. Sendo o crachá pessoal e intransferível, não deve ser entregue ou emprestado a outros colaboradores ou terceiros.

Não é permitido deixar os crachás disponíveis em locais públicos e ao sair das dependências do Finaxis, o mesmo deverá ser guardado em local seguro de forma que um funcionário ou prestador de serviços não seja identificado fora das dependências das empresas Finaxis.

Este procedimento tem por objetivo resguardar os colaboradores e a empresa de pessoas mal-intencionadas.

O acesso de visitantes às dependências do Finaxis deverá sempre ocorrer após a autorização de um funcionário e sempre acompanhado do mesmo.

Prestadores de Serviços e suas respectivas empresas deverão assinar um termo de confidencialidade sempre que forem desempenhar alguma atividade na qual venham a ter acesso às informações do Finaxis, ou possuir cláusula específica no contrato de prestação de serviço que trate sobre a confidencialidade e a ciência e aderência a esta Política.

As áreas de processamento de informação deverão ter acesso restrito e controlado conforme o nível de confidencialidade das informações processadas, ao final do expediente as salas devem ser trancadas.

Os ambientes da estrutura do Finaxis podem ser filmados as imagens serão preservadas pelo Finaxis, podendo ser utilizadas nos termos da lei.

3.4. Uso de Impressoras

Todos os colaboradores devem utilizar senha de acesso para a impressão de documentos confidenciais quando disponível e, não sendo possível, recolher o material impresso de imediato. Todo o funcionário que constatar irregularidades na utilização da impressora deve comunicar o fato ao seu gestor, à área de Segurança da Informação ou ao Compliance, que tem autonomia para destruir o que foi encontrado e não

retirado da impressora, além de informar o superior hierárquico do infrator. Só imprimir quando necessário.

3.5. Ciclo de Vida

Toda informação possui um ciclo de vida que é dividido em três partes distintas: Criação, Transporte e Descarte.

Durante a criação da informação, o proprietário é responsável por rotulá-la e classificá-la de acordo com seu grau de confidencialidade, aplicando controles proporcionais aos riscos que estas informações representam para as empresas Finaxis, em caso de comprometimento de um ou mais princípios da Segurança da Informação.

Para o transporte, seja ele físico ou lógico, ou qualquer outro meio para tráfego de informações, este também deverá refletir os controles proporcionais à classificação da Informação e aos riscos inerentes, lembrando que o transporte de informações Sensíveis ou Confidenciais, deverá ocorrer sempre em meio seguro de forma a garantir sua confidencialidade conforme procedimento específico para transporte e salvaguarda de informações a ser implementado.

O descarte é o processo final no ciclo de vida de uma informação e alguns cuidados devem ser seguidos conforme abaixo:

- **Documentos que contenham informações confidenciais**, sensíveis e privado, devem ser destruídos nas fragmentadoras de papéis disponíveis no prédio ou colocados em locais para armazenar e posterior fragmentação.

- **Os documentos com informações classificadas como publica** podem ser utilizadas como rascunhos, e as mídias devem ser devolvidas a área de Tecnologia da Informação para o correto descarte e destruídas de forma que seu conteúdo não possa ser recuperado, respeitando-se a classificação de informações tratada no item 4.1.

- Os equipamentos devolvidos à área de Tecnologia da Informação – Infraestrutura serão formatados por esta, sendo entregues a usuários posteriores sem informações geradas por outros usuários.

3.6. Utilização de Softwares

Os funcionários devem utilizar apenas os softwares instalados pela equipe de tecnologia da informação, que encontram-se devidamente registrados e licenciados pela instituição, existindo um padrão de software que deve ser obedecido por todos os funcionários. Não é permitido o uso ou instalação de programas que não foram adquiridos, homologados e licenciados pelo Finaxis.

Havendo necessidade de aquisição ou desenvolvimento de um software ou aplicativo, a área usuária deverá encaminhar solicitação à área de Tecnologia da Informação, que procederá às análises de viabilidade e autorizações necessárias, incluindo a área de Segurança da Informação.

3.7. Uso de Correio Eletrônico (E-mail)

O e-mail se limita exclusivamente aos negócios das empresas do Finaxis não podendo nenhuma mensagem conter comentários abusivos, obscenos ou difamatórios ou qualquer outro material que possa trazer má publicidade ou constrangimento público ao Finaxis, seus clientes ou prestadores de serviços.

Deve-se evitar a utilização do e-mail para troca de mensagens confidenciais ou estratégicas para os negócios da instituição. Quando necessário, a mensagem deverá ser tratada com extremo caráter de confidencialidade.

O e-mail corporativo constitui ferramenta disponibilizada para o desenvolvimento das funções do colaborador, sendo as mensagens neste trafegadas, monitoradas pela área de Segurança da Informação. Portanto, seus colaboradores devem estar cientes de tal monitoramento, sendo, entretanto preservada sua privacidade, em decorrência do caráter estritamente confidencial deste procedimento.

3.8. Mesa limpa

O colaborador deverá sempre bloquear seu computador ao deixar a estação de trabalho, ainda que momentaneamente e não deverá deixar informações sensíveis ou confidenciais disponíveis ao alcance de outras pessoas.

Ao final do expediente, todo colaborador deverá guardar seus documentos em local fechado com chave e desligar sua estação de trabalho, a fim de deixar a sua mesa limpa e sem nenhum tipo de informação disponível.

Deve-se, ainda, manter os armários e gaveteiros devidamente trancados, evitando assim o acesso indevido a informações da instituição.

3.9. Dispositivos móveis

A utilização de dispositivos móveis e de gravação (Pen drives, Placas 3G ou Celulares para acesso a Internet, Leitores de Cds, entre outros) nos ativos da instituição não é permitida. Em casos excepcionais em que seja necessário o uso em decorrência de atividade ou situação específica, o colaborador deverá enviar solicitação à área de Segurança da Informação, contendo aprovação do diretor da área, aguardando análise e aprovação da mesma. Estes equipamentos não poderão ser utilizados como alternativa de cópia de segurança (backup).

Apenas os equipamentos e softwares disponibilizados e homologados pelo Finaxis serão permitidos em suas dependências.

Equipamentos pessoais de funcionários e prestadores de serviço, devem estar abrangidos no termo de confidencialidade ou na clausula de confidencialidade do contrato de prestação de serviço e deverão ter sua conexão de rede controlado e restringida. Caso contrário não tem o uso autorizado.

3.10. Sistemas de Informações

Os sistemas e aplicativos, desenvolvidos internamente ou por terceiros deverão estar em conformidade com os requisitos de Segurança da Informação.

Todos os sistemas de informação do Finaxis devem possuir um gestor de sistemas responsável, com cargo mínimo de gerente e um suplente (backup) indicado pelo gestor principal, podendo ser um coordenador

Os gestores têm a responsabilidade de definir a correta utilização e segurança do sistema, autorizando o acesso de outros colaboradores por meio de perfis de acesso pré-definidos, garantindo a segregação de funções, partindo da premissa de autorizar os acessos estritamente necessários para o desempenho das atividades e de acordo com a alçada do funcionário. Cabe ainda ao gestor responsável realizar revisões periódicas nos acessos concedidos e revogar de imediato os acessos com poderes excessivos ou desnecessários, conforme classificação da informação do sistema.

3.11. Logins e senhas de acesso

Todos os logins e senhas de autorização de acesso aos sistemas de informação são pessoais e intransferíveis e todos os colaboradores usuários têm o dever e a responsabilidade de proteger, não divulgar e utilizar única e exclusivamente para o fim que foi autorizado.

As ações decorrentes da utilização destes poderes são de inteira responsabilidade do usuário, portanto, nenhuma pessoa, ainda que gestor ou superior hierárquico, está autorizado a solicitar a senha de um colaborador. Em ocorrendo tal solicitação, o colaborador deverá comunicar o fato à área de Segurança da Informação, para providências cabíveis, sendo preservado o sigilo na comunicação do fato.

O compartilhamento de senhas entre usuários constitui falta grave, podendo sujeitar os colaboradores às sanções dispostas no Código de Ética e Conduta da instituição.

Os acessos aos sistemas de informação e redes de computadores são revisados periodicamente conforme procedimento: “06 Procedimento de Revisão de Acessos”.

3.12. Recursos de rede

A utilização de recursos de rede, incluindo a utilização do correio eletrônico e o acesso à Internet tem a finalidade única e exclusiva de atender aos interesses do negócio devendo respeitar as diretrizes desta política e demais Políticas do Finaxis que tratam estes assuntos.

O acesso remoto aos recursos de sistemas e rede deve ser liberado somente após solicitação formal do Diretor do ativo que deve avaliar a solicitação e justificativa do acesso, antes de formalizar a respectiva autorização. Estes acessos só podem ser efetuados por meio de equipamentos homologados, autorizados e que atendam aos requisitos de segurança.

O acesso remoto realizado por empresas parceiras, deverá estar em conformidade com esta política e estará sujeito à análise prévia dos requisitos de segurança do Finaxis, bem como definição de responsabilidade em cláusula especifica do contrato de parceria.

O acesso à Internet deve estar de acordo com o procedimento: " 07 Utilização de Internet " do Finaxis, sendo proibido o acesso a qualquer conteúdo que viole a ética, as diretrizes e as políticas do mesmo.

O acesso à Internet através da rede do Finaxis só será concedido mediante autenticação do usuário e senha, e todo e qualquer acesso será monitorado.

Nos diretórios e pastas da rede não é permitido salvar arquivos de Fotos (JPEG, JPG, TIF, .BMP, Etc...), Músicas (MP3,MP4, Etc...), Filmes(WMA, AVI, MPEG,DIVXX, etc...), exceto quando os mesmos são indispensáveis para o desenvolvimento das atividades da área ou de algum profissional específico.

3.13. Comunicação

O fornecimento de informações da empresa a terceiros, quando necessário, deve ser realizado com extremo cuidado, sempre buscando assegurar que a pessoa que está recebendo a informação seja o destinatário correto e que esta informação não traga prejuízos ao Finaxis. Havendo dúvidas, não forneça a informação e contate as áreas de Compliance e Jurídico que estão preparadas para ajudá-lo.

3.14. Monitoramento

As ações decorrentes da utilização dos ativos do são de inteira responsabilidade do usuário e poderão ser monitoradas, coletadas e utilizadas a critério do Finaxis para a execução de investigações internas ou atendimento de medidas judiciais, sem o prévio aviso aos envolvidos, respeitando, porém, a privacidade de seus funcionários e colaboradores.

Para garantir a conformidade, alguns dos ramais telefônicos do Finaxis tem suas ligações gravadas, de acordo com o procedimento: "09 Utilização de Sistemas de Telefonia".

4. SANÇÕES

O descumprimento de quaisquer dispositivos estabelecidos na presente política e nos demais documentos que suportam sua implementação acarretará na imposição de sanções a serem definidas pelo Comitê de Ética e Conduta, sendo cabíveis ainda as penalidades descritas na legislação vigente.

5. TERMO DE COMPROMISSO

Todos os colaboradores e prestadores de serviços que utilizam nossas informações devem formalizar o conhecimento e aceitação desta política através da assinatura do Termo de Compromisso (Anexo).

Os termos firmados permanecerão arquivados junto à área de Gestão Estratégica de Pessoas, quando dos colaboradores, e pela área Jurídica junto aos contratos de prestação de serviço.

6. VIGÊNCIA

Esta política entra em vigor na data de sua publicação e permanece vigente por tempo indeterminado.

7. ANEXOS

7.1. Anexo I

TERMO DE COMPROMISSO

Declaro haver recebido nesta data uma cópia da Política de Segurança da Informação do Finaxis, para minha informação e uso pessoal.

Declaro conhecer integralmente o conteúdo da Política de Segurança da Informação e seus Procedimentos.

Declaro estar informado(a), e ciente com o fato, de que a Política de Segurança da Informação do Finaxis faz parte dos termos do meu vínculo empregatício ou de prestação de serviços de qualquer natureza com a Finaxis.

Declaro ainda, ser de minha responsabilidade ler, entender e me manter atualizado(a) sobre as regras e obrigações descritas nesta Política e nos Procedimentos a ela vinculados; buscando, sempre que necessário; esclarecimento ou mais informações e estando sempre em conformidade com os conteúdos daquele documento.

Declaro entender que toda infração à Política resultará em medida disciplinar que pode incluir o término do meu vínculo empregatício ou de prestação de serviços de qualquer natureza com a Finaxis.

Declaro reconhecer que posso, a qualquer momento, sanar dúvidas a respeito da Política.

_____, ____ de _____ de _____

Nome (em letra de forma): _____

Assinatura: _____

7.2. Anexo II

UTILIZAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA E ACESSOS

Eu, abaixo assinado, declaro nesta data, ter ciência e estar de acordo com os procedimentos descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente. Conheço minhas responsabilidades enquanto usuário de TI desta Empresa citadas na Instrução Normativa de TI e detalhadas neste Termo, conforme segue:

a. Os equipamentos de informática e acessos de usuário que foram a mim fornecidos são instrumentos de trabalho que têm como objetivo melhorar o desempenho das funções para as quais eu fui contratado;

b. Recebido tais equipamentos e acessos, sou responsável pela utilização dos mesmos, bom como dos acessórios (monitor, teclado, mouse, unidades de CD/DVD, etc.);

c. Se por razões de trabalho, houver necessidade de mudar a localização física, solicitar formalmente à Área de TI, que é o único departamento autorizado a realizar a circulação física dos equipamentos;

d. Devo utilizar a caixa postal (e-mail) colocada a minha disposição e acessar a Internet/Intranet somente por necessidade de serviço ou por determinação expressa de superior hierárquico. Da mesma forma, realizar as atividades em estrita observância aos procedimentos, normas e disposições que regem o acesso a Internet/Intranet e utilização de e-mails;

e. Tenho conhecimento dos procedimentos e normas de TI, e quando da ausência de conhecimento dos mesmos, sei que devo buscar esclarecimentos com a área de TI da empresa;

f. Não devo revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

g. Devo manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

h. Não devo ausentar-me da estação de trabalho sem encerrar/bloquear a sessão de uso do navegador (browser), bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

i. Não devo revelar minha senha de acesso a Internet/Intranet e de minha caixa postal (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

j. Responderei, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso;

k. Não é permitido utilizar o computador para executar quaisquer tipos ou formas de fraudes, ou software/música pirata;

l. Não é permitido utilizar a Internet para enviar material ofensivo ou de assédio para outros usuários;

m. Não é permitido baixar (download) software comercial ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento ou outros tipos de licença;

n. Não é permitido atacar e/ou pesquisar áreas não autorizadas (*Hacking*);

o. Não devo criar nem transmitir material difamatório;

p. Não devo executar atividades que desperdicem os esforços do corpo técnico ou dos recursos da rede;

q. Não devo introduzir de qualquer forma um vírus de computador dentro da rede corporativa.

Declaro, ainda, estar plenamente esclarecido e consciente que:

a. Não é permitida a navegação em sites pornográficos, defensores do uso drogas, de Pedofilia ou sites de cunho racista e similares;

b. É minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade das informações contidas em minha caixa postal (e-mail), devendo comunicar por escrito à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas no sistema de correio, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

c. O acesso à informação de minha caixa postal (e-mail) não me garante direito sobre ela, nem me confere autoridade para liberar acesso a outras pessoas, pois se constitui informações pertencentes da administração, uma vez que faço uso para melhor desempenhar minhas atividades administrativas;

d. Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos por meio do uso de minha caixa postal (e-mail);

e. Devo alterar minha senha, sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

f. Devo respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição;

g. Cumprir e fazer cumprir os dispositivos da Política Corporativa de Segurança da Informação, de suas diretrizes, bem como deste Termo de Responsabilidade. Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional a revelação de segredo do qual me apropriei em razão do cargo e a divulgação a quem não seja funcionário da empresa, das informações a (s) qual (is) tenho acesso, estando sujeito às penalidades previstas em lei;

Sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda que habilitado;

Constitui infração funcional e penal enviar ou facilitar o envio por terceiros de e-mails falsos, ficando o infrator sujeito a punição com a demissão, conforme responsabilização por crime, tipificado no art. 313-A e 313-B, do Código Penal Brasileiro (Decreto-Lei 2.848, de 1940).

MONITORAMENTO

A Empresa reafirma que o uso da Internet é uma ferramenta valiosa para seus negócios. Entretanto, o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade dos funcionários e a própria reputação do negócio.

Em adição, todos os recursos tecnológicos da Empresa existem para o propósito exclusivo de seu negócio.

Portanto, a Empresa se dá ao direito de monitorar o volume de tráfego na Internet e na Rede, juntamente com os endereços web visitados.

Tentativas de burlar tais sistemas de monitoramento serão consideradas infrações das Normas da Empresa.

O descumprimento de qualquer um dos itens citados pode gerar punições, conforme a gravidade da conduta, e/ou o histórico funcional do colaborador e/ou demais critérios definidos na legislação vigente, podendo, inclusive, levar a rescisão do contrato de trabalho do colaborador por justa causa.

_____, _____ de _____ de _____.

Nome do Funcionário: _____

Cargo do Funcionário: _____

I.d. de acesso: _____

Assinatura: _____

7.3. Anexo III

SIGILO DA INFORMAÇÃO

Eu, _____, portador do CPF_____, declaro que estou ciente das políticas e procedimentos de segurança da informação do Finaxis e afirmo meu compromisso em segui-las, estando ciente, principalmente que:

• Todas as informações geradas no ambiente de trabalho são de propriedade do Finaxis, dessa forma é expressamente proibido o envio de informações e/ou documentos de caráter funcional do e-mail corporativo para e-mail pessoal;

• Todas as ações realizadas por mim na empresa, podem e devem ser monitoradas no sentido de garantir a segurança das informações e minimizar o risco de acesso indevido a elas;

• O não cumprimento de quaisquer itens acima e/ou das políticas e procedimentos de segurança da informação, podem gerar sanções administrativas, que vão desde uma advertência verbal até demissão por justa causa, de acordo com a gravidade do desvio à política realizado.

Eu me responsabilizo integralmente e a qualquer tempo pela adequada utilização das informações a que tiver acessos. Inclusive a partir do momento que não mais fizer parte do quadro de colaboradores do Finaxis.

_____, _____ de _____ de _____.

_____

Assinatura