POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POL-0401
DATA 16/05/2023

ideal

1 Abrangência

Esta Política é aplicável aos Colaboradores Internos, prestadores de serviço e fornecedores da Corretora que tenham acesso ao ambiente tecnológico e à rede da Corretora.

2 Alçada de aprovação

- A subárea de Segurança da Informação é responsável pela elaboração, manutenção, revisão e implementação desta Política e suas versões; e
- Compete ao superintendente de Tecnologia da Informação e à Diretoria a aprovação desta Política e de suas versões revisadas.

2.1 Violações

- Compete à área TI administrar e efetuar a gestão das situações de inadimplência com as regras de segurança da informação estabelecidas nesta Política, escalando ao Compliance e à Diretoria, conforme aplicável;
- Compete ao superintendente de tecnologia da informação juntamente com a Diretoria a definição e a execução de ações voltadas tanto para a correção como para a prevenção das violações identificadas; e
- A transgressão aos preceitos do COD0001 – Ética e Conduta, e aos documentos corporativos, conforme o grau de severidade, poderão resultar em advertência, suspensão ou demissão conforme disposto nos Documentos Corporativos da Corretora, além das penalidades legais aplicáveis.

3 Revisão da Política

A revisão desta Política deverá ser realizada no mínimo a cada 2 (dois) anos, ou em menor periodicidade se assim requerido pela Diretoria ou pelas áreas de TI e/ou Compliance.

3.1 Histórico de revisão

Revisor	Data	Descrição
Fabio Farias	01/11/2018	Versão inicial
Fabio Farias	26/06/2019	Inclusão do capítulo de “Segurança no descarte de material impresso” Inclusão do capítulo de “Segurança no descarte de mídias físicas e equipamentos de TI”
Fabio Farias	29/10/2019	Revisão Anual Inclusão do capítulo “Escaneamento de Vulnerabilidades” Alteração na Política de Senhas Alteração no Uso de Internet Alteração nos Acessos Lógicos
Peter Klein	31/10/2019	Ajustes periféricos e revisão das inclusões.

Diretoria	05/11/2019	Aprovação versão 2.0
Fabio Farias	29/07/2020	Incorporação das diretivas da política de segurança cibernética e sistematização de uma gestão integrada das disciplinas. Reorganização geral dos assuntos e adaptações à luz da ICVM 612. Alteração no leiaute do documento em adequação ao novo sistema visual da marca
Peter Klein	11/08/2020	Revisão das alterações promovidas por TI
Diretoria	31/08/2020	Aprovação versão 3.0
Fabio Farias	04/12/2020	Adição de critérios para contratação de serviços em nuvem
Lucas Cury	09/12/2020	Detalhamento e diferenciação entre critérios de decisão e requisitos de contratação de serviços em nuvem.
Márcio Ramalho	26/10/2021	Revisão Anual 2021
Peter Klein	25/11/2021	Revisão das alterações promovidas por TI – versão 6.0
Diretoria	01/12/2021	Aprovação versão 6.0
Thais Devides	06/07/2022	Revisão do formato da Política e reorganização das diretrizes. A partir desta versão passou a se tratar a matéria de SI de forma independente retomando a sua contagem a partir da versão 3.0 em linha com o banco de Políticas da Corretora.
Diretoria	16/05/2023	Aprovação da versão 3.0 da POL0401 – Segurança da Informação (desmembrada).

4 Glossário

Termo	Descrição
Anonymizer ou Anonymizer proxy	Software ou serviço instalado localmente ou utilizado na Internet com o objetivo de impedir rastreabilidade de navegação na Internet
Ativos de Informação	Os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
Computação em Nuvem	Ambiente de infraestrutura lógica, que hospeda infraestrutura de servidores e demais serviços. Este ambiente é virtualizado e replicado em Data centers físicos situados em diversos locais.

Dados Sensíveis	São os dados que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa
Dados Pessoais	Informação Pessoal Identificável (dado pessoal e sensível) é toda e qualquer informação que separada ou em conjunto pode levar a identificação da pessoa física, seja ela cliente, fornecedor ou colaborador. Exemplos são números de documentos (RG, CPF etc.), números de contas correntes ou de negociação, endereços, e-mail, posições em custódia e outros.
PSI ou Política	Política de Segurança da Informação
Sistemas Críticos	Sistemas que tem sua função principal o suporte aos processos de negociação, custódia e liquidação ou que auxiliam estes sistemas.
TSI	Departamento de Tecnologia e Segurança da Informação

5 Objetivo – Política de Segurança da Informação

A Política de Segurança da Informação – PSI tem como objetivo estabelecer as diretrizes, orientações e responsabilidades relativa à proteção da informação e proteger os 3 (três) pilares de segurança: Confidencialidade, Integridade e Disponibilidade.

Também se destina a atender os requisitos da Resolução BCB Nº 4.557 e suas alterações, que dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital, no que diz respeito à estrutura de sistemas, processos e infraestrutura de tecnologia da informação, bem como demais normas que dispõem sobre requisitos de segurança da informação.

6 Diretrizes

As seguintes diretrizes deverão ser observadas de forma contínua a partir dos 3 pilares de segurança da informação e privacidade:

Confidencialidade: Assegurar que o acesso as informações sejam feitas somente por pessoas autorizadas.

I. Proteger os dados e sistemas contra acessos indevidos, implementando controles de acesso e autorização, conforme o princípio de *need-to-know* definidos em políticas ou manuais específicos para este fim;

II. Implementar mecanismo de identificação da identidade dos usuários por meio de utilização de múltiplos fatores de autenticação e definir parâmetros mínimos de senhas conforme aplicável e definido no Manual de Controle de Acesso;

III. Definir claramente os responsáveis pelas aprovações de acesso, que devem, no mínimo, ser aprovadas pelo gestor e pelo dono do sistema;

IV. Criptografar dados e informações em trânsito e em descanso, incluindo cópias de segurança (Backup), em todo ambiente da corretora de acordo com padrões de criptografia definidos nas melhores práticas dos principais institutos de padronização de computação (ex.: NIST);

V. Manter de forma segura, a guarda das chaves de criptografia e certificados digitais para acesso aos recursos computacionais, elaborando processos e procedimentos adequados para sua guarda, renovação, revogação e inutilização, além de manter registro;

VI. Antes da contratação de qualquer fornecedor, seja ele relevante ou não deve ser preenchido o formulário de Gestão de Fornecedor;

VII. Controlar o acesso físico e lógico ao ambiente e dispositivos da Corretora, adotando mecanismos de segurança de modo a evitar ameaças a sua confidencialidade e integridade conforme controle de autorização e autenticação adotados e definidos no Manual de Controle de Acesso; e

VIII. Descartar equipamentos e documentos adequadamente de forma a evitar vazamento de dados pessoais, restritos ou confidencias em linha com as diretrizes do Manual de Descarte de Equipamentos e Política de Classificação de Dados;

Integridade: Salvaguardar com exatidão e completude as informações, tal como foram criadas ou recebidas.

I. Manter cópias de segurança dos dados da corretora (bancos de dados, sistemas, logs, trilhas de auditoria) pelos prazos definidos pelas leis e regulamentações aplicáveis, em local diferente dos ambientes produtivos, definindo os processos e procedimentos em manual específico para este fim;

II. As cópias de segurança devem ser testadas regularmente para garantir que estão integras e o processo deve ser detalhado em manual específico;

III. Manter trilhas de auditoria das ações executadas em ambientes produtivos permitindo a rastreabilidade de quem, quando, o que, onde e por que das alterações efetuadas;

IV. Garantir a imutabilidade das trilhas de auditoria dos sistemas produtivos; e

V. Manter catálogo dos dispositivos e sistemas especificando suas principais características: Nome, descrição, dono do sistema, dono dos dados do sistema, responsável técnico e outras que sejam necessárias conforme entendimento da equipe de Tecnologia da Informação.

Disponibilidade: Assegurar que o acesso à informação pertencente ao ecossistema tecnológico esteja disponível sempre que necessário pelos usuários.

I. Garantir a continuidade de seus negócios por meio da elaboração de um plano que seja exequível e testado, ao menos, anualmente, detalhados em Documentos Corporativos específicos para esta atividade;

II. Monitorar ativamente a capacidade dos sistemas e equipamentos de modo a prevenir indisponibilidade em caso de demandas excessivas;

III. Executar testes de estresse dos sistemas e dispositivos periodicamente, no mínimo a cada ano, conforme Documentos Corporativos aplicáveis;

IV. Investir continuamente em aprimoramentos de tecnologia que assegurem a perenidade das premissas de segurança de informação e segurança cibernética;

V. Todos os sistemas e dispositivos produtivos devem ser monitorados quanto a sua saúde (quantidade de memória, CPU, espaço em disco, consumo de rede e disponibilidade); e

VI. Monitorar, identificar, registrar, acompanhar e resolver incidentes em ambiente produtivo, mantendo a disponibilidade adequada dos sistemas e serviços da corretora, conforme Documento Corporativo relativo à Gestão de Incidentes e Problemas.

Privacidade e Proteção de Dados Pessoais: Assegurar que os dados pessoais contidos nas informações são protegidos com a adoção de medidas técnicas e organizacionais de Segurança da Informação.

I. Tratar de maneira ética e sigilosa, as informações de clientes, usuários, parceiros, fornecedores e Colaboradores;

II. É vedado a qualquer indivíduo à utilização indevida e/ou o compartilhamento de informações da Corretora a pessoas não autorizadas;

III. Os Colaboradores Internos devem assinar o Termo de Confidencialidade no ato da admissão; e

IV. As informações geradas ou recebidas externamente (apresentações, e-mails, textos, planilhas etc.) devem ser classificadas de acordo com os Documentos Corporativos relativos à classificação de dados.

Conscientização e divulgação: Disseminar continuamente aos Colaboradores Internos e terceiros as Documentos Corporativos e diretrizes de segurança da informação, buscando, dentre outros pontos a implementação das seguintes ações:

I. Capacitar tecnicamente e conscientizar constantemente os Colaboradores Internos e terceiros que possuam acesso ao ambiente tecnológico;

II. Disseminar o Programa de Conscientização continuamente de forma a capacitar os Colaboradores Internos;

III. Fornecer treinamento de conscientização de segurança anualmente;

IV. Monitorar a adoção de mecanismos que certificam a leitura, por parte dos Colaboradores Internos, do treinamento de Segurança da Informação bem como desta Política;

V. Avaliar por meio de testes e simulados a aderência dos Colaboradores Internos e terceiros aos treinamentos e campanhas do programa de conscientização e definir a necessidade de recertificação se aplicável;

VI. Disseminar esta Política a todos os envolvidos na operação da Corretora, sejam eles Colaboradores Internos ou terceiros, conforme aplicável;

VII. Comunicar os Colaboradores Internos no início de suas contratações e anualmente, ou em caso de atualização, conforme necessário; e

VIII. Informações exigidas por lei ou regulamentação relativas à negociação de valores mobiliários devem ser gravadas e mantidas pelos prazos definidos na regulamentação vigente, garantindo sua integridade e disponibilidade e permitindo a identificação das pessoas envolvidas e a data e hora das mensagens;

IX. Os contratos com as partes externas que apresentem serviços ou risco relevante de SI devem possuir cláusulas que assegurem as obrigações em cumprir com os requisitos e diretrizes de segurança da informação;

X. Utilizar os recursos tecnológicos da Corretora, como e-mail, softwares de mensagem instantânea, computadores e celulares de acordo com o uso previsto nos Documentos Corporativos referentes ao uso aceitável das ferramentas da Corretora; e

XI. As informações devem ser classificadas de acordo com o Documento Corporativo de Classificação.

7 Papeis e responsabilidades

Compete à Diretoria:

I. Aprovar a PSI e suas revisões;

II. Tomar decisões administrativas em casos de descumprimento desta PSI, quando demandada; e

III. Promover o ambiente necessário e fornecer os recursos necessários para assegurar o programa de segurança da informação da Corretora.

Compete às Gerências:

I. Assegurar o cumprimento e ciência desta PSI com suas respectivas equipes;

II. Assegurar, em conjunto com a área de Tecnologia da Informação, que os requisitos desta PSI e demais Documentos Corporativos de segurança sejam cumpridos em seus processos; e

III. A contratação de serviços relevantes em nuvem ou não, que suportem sistemas críticos e/ou Dados Pessoais ou Sensíveis, deve levar em consideração os requisitos mínimos que a contratada deve atender durante a prestação dos serviços, além do preenchimento do formulário de Gestão de Fornecedores e ser avaliado antes da contratação.

Compete à subárea de Segurança da Informação:

I. Apoiar nos processos de gestão de riscos e controles internos, no que se refere a avaliação dos riscos de segurança da informação e definição dos controles e ações de melhorias necessárias;

II. Manter o Programa de Conscientização de segurança da informação ativo e realizar sua revisão e reciclagem anualmente;

III. Atualizar esta PSI e demais Documentos Corporativos de segurança da informação; e

IV. Comunicar à área de Compliance, em caso de novas políticas ou nomas.

Compete à área de Tecnologia da Informação

I. Manter cópias de segurança de dados e logs de acesso físico e lógico armazenadas de acordo com o período requisitado pela norma aplicável (seja esta lei ou regulamentação);

II. Documentar processo de guarda, renovação, revogação e inutilização de certificados digitais

III. Manter registro de todas as chaves de criptografia e Certificados Digitais existentes, informando o dono e o mantenedor.

IV. Dar suporte ao Proprietário da Informação na identificação das atividades executadas pelos colaboradores para apoiar no processo de segregação de funções;

Compete a área de Compliance:

I. Comunicar aos Colaboradores Internos quanto a disponibilização de versões revisadas ou novos Documentos Corporativos; e

II. Publicar na página do SharePoint de Governança (interno) os Documentos Corporativos novos ou atualizados. Fazer a manutenção da base de Documentos Corporativos da Corretora, revogando as versões vencidas e modificadas sempre que necessário por conta de prazo de vigência, mudança legal ou regulatória ou solicitação da área responsável.

Compete a área de Recursos Humanos:

I. Disponibilizar a PSI e demais documentos Corporativos aos novos Colaboradores Internos e armazenar os respectivos registros;

II. Armazenar os documentos assinados de segurança da informação na ficha do colaborador que atestam a ciência referente aos processos de segurança da informação; e

III. Informar as alterações de Colaboradores Internos às áreas de TI e Segurança da Informação (admissão, transferências, afastamentos, licenças e desligamentos).

Compete aos Colaboradores:

I. Preservar a confidencialidade, integridade e disponibilidade da informação e de seus ativos;

II. Não expor, compartilhar ou discutir informações internas da Corretora em ambientes públicos (meios de transporte, aeroportos, elevadores, restaurantes, mas não limitado a estes);

III. Não emitir comentários, opiniões referentes a informações da Corretora em redes sociais, blog ou até mesmo para imprensa;

IV. Nunca compartilhar ou divulgar suas credenciais, como login e senha, mesmo que seja com Colaboradores Internos, pois elas são pessoais, individuais e de sua responsabilidade; e

V. Comunicar imediatamente a subárea de Segurança da Informação em caso de qualquer violação desta PSI ou demais Documentos Corporativos de segurança da informação.

8 Objetivo – Uso aceitável

Este tópico referente ao Uso Aceitável tem como objetivo estabelecer regras de utilização de ativos afim de proteger as informações e que seu uso seja feito de forma eficaz, ética, lícita e transparente.

9 Diretrizes

Em relação às regras desta Política, as seguintes diretrizes deverão ser observadas de forma contínua:

I. Colaboradores Internos devem dispor apenas dos recursos tecnológicos necessários e devidamente homologados para exercer suas atividades;

II. Nenhuma atividade tecnológica deve ser executada fora do ambiente interno (VPN – *Virtual Private Network* – Rede Privada Virtual ou AWS – *Thin Client*) da Corretora;

III. Os recursos cedidos devem ser utilizados apenas para o proposito para o qual ele foi autorizado, inclusive a credencial de acesso;

IV. Os ativos (computador, celular e notebook) devem ser configurados com os requisitos básicos de segurança:

- Antivírus atualizado e ativado;
- Controle de acesso à internet
- Atualização de segurança ativado e com instalações recentes.

V. O armazenamento na rede (*sharepoint, one drive*) de informações pessoais é proibido. Para fins pessoais é aceitável a utilização do disco local, seguindo as seguintes moderações:

- É terminantemente proibido o armazenamento de músicas, vídeo e fotos, exceto aqueles vinculados as atividades profissionais;
- Não comprometer o desempenho dos sistemas da Corretora;
- Não for utilizado de forma incompatível em atividades paralelas ou para fins ilícitos; e
- Não contrariar legislações vigentes ou Documentos Corporativos da Corretora.

VI. Os acessos podem ser registrados e gerar relatórios dos sites visitados, *downloads* efetuados, tempo de acesso, informação consultada, entre outros; e

VII. É proibido conectar mídias removíveis nos equipamentos fornecidos pela Corretora, exceto mediante autorização formalizada da área de Segurança e do respectivo Gestor.

10 Uso de equipamentos

Os equipamentos disponibilizados pela Corretora são de uso exclusivo para atividades da empresa:

I. É vedado sua utilização para atividades não relacionadas, sendo dever dos Colaboradores empreenderem todos os esforços pelo uso racional dos equipamentos colaborando com a extensão de sua vida útil;

II. As estações de trabalho deverão estar sempre bloqueadas quando não estiverem sendo utilizadas;

III. Todo e qualquer equipamento eletrônico utilizado nas dependências da Corretora deverá ser de conhecimento e consentimento da área de TI e de Segurança da Informação, sendo vedado a conexão de aparelhos não autorizados em sua rede de comunicações;

IV. Apenas equipamentos fornecidos pela Corretora podem ser conectados à rede corporativa;

V. Equipamento de uso pessoal podem ser conectados à rede sem fio especificas; e

VI. É proibido uso de dispositivos móveis de armazenamento, com exceção de casos com aprovação da área de Segurança da Informação e abertura de chamado.

11 Instalação e utilização de softwares

I. Somente softwares homologados e autorizados pelas áreas de TI e TSI, poderão ser instalados e utilizados;

II. Somente a área de TI está autorizada a testar e homologar novos softwares; e

III. É proibido o uso de softwares ilegais ou em não-conformidade com a licença de uso do software.

12 Uso do correio eletrônico e mensagens instantâneas

O correio eletrônico é um instrumento de comunicação interna e externa cujo objetivo é viabilizar a execução das atividades corporativas. Referida ferramenta é monitorada com o intuito de bloquear o vazamento de dados e informações, spams, vírus ou outros conteúdos maliciosos. O uso de referida ferramenta, deve observar, dentre outros requisitos, as seguintes regras:

I. O acesso ao correio eletrônico deve ser concedido somente aos Colaboradores Internos que necessitam desse recurso para desempenhar as atividades profissionais respectivas;

II. Somente aplicativos e sites aprovados e homologados pelas áreas de TI e TSI, devem ser utilizados para troca de mensagens instantâneas; e

III. Seu uso é pessoal sendo o usuário responsável por toda e qualquer mensagem enviada pelo seu endereço.

É proibido rigorosamente:

I. Falsificar, obscurecer, suprimir ou substituir a identidade de um usuário no sistema de correio eletrônico ou adulterar ou falsificar mensagens de correio eletrônico;

II. Enviar mensagens eletrônicas com informações classificadas como confidenciais para endereços externo do domínio da empresa, exceto quando necessário para alguma atividade de negócio e utilizando os recursos de segurança indicados pela área de Segurança da Informação;

III. Abrir mensagens ou arquivos com origem desconhecida;

IV. Enviar mensagem com anúncios de eventos particulares, propagandas, opiniões pessoais, vídeos, músicas, campanhas ou promoções;

V. Utilizar o e-mail corporativo para participação de fóruns e lista de discussão ou cadastro em sites de comércio eletrônico, redes sociais entre outros não se limitando a estes ou não relacionados ao negócio ou para assuntos pessoais; e

VI. Envio de e-mail em massa, exceto quando seu uso for para atividades do negócio e deve ser realizado com orientação da área de Segurança da Informação;

É proibido também a utilização do correio eletrônico para enviar, receber ou manter armazenadas mensagens com:

I. Sexo, educação sexual, erotismo, pornografia e pedofilia;

II. Sons, imagens ou vídeos que não estejam relacionados aos negócios do Grupo Ideal;

III. Propaganda política;

IV. Assuntos de cunho religioso, racial, sexual, preconceituoso ou apologia a qualquer atividade ilegal

V. ou ofensiva;

VI. Arquivos contendo jogos; e

VII. Correntes ou qualquer tipo de propaganda que possa ser considerada “spam”.

13 Uso da internet

I. O acesso à Internet é autorizado para os usuários conforme a necessidade para o desempenho de suas atividades na Corretora;

II. Os Colaboradores Internos e terceiros que fazem uso da internet corporativa da Corretora, devem ter ciência que estes acessos são constantemente monitorados e auditados e que devem ser utilizados apenas para o uso profissional;

III. Cada Colaborador Interno terá associado ao seu login de acesso um perfil para acessar a internet, previamente estabelecido para o desempenho de suas funções, caso necessite de acesso adicional este deve ser realizado através de chamado para a área de TI, com as aprovações da área de TSI e do seu gestor direto; e

IV. O acesso a redes sociais é autorizado, mediante aprovação de Segurança da Informação e Compliance, exclusivamente para atividades relacionadas ao negócio da empresa.

É vedado o acesso à internet para:

I. Instalação de programas provenientes da Internet nos computadores da Corretora, sem expressa anuência das áreas de TI e TSI;

II. Visualização, transferência (downloads e/ou uploads), cópia ou qualquer outro tipo de acesso a sites:

III. Acesso de sites de conteúdo adulto (sexo, erotismo, educação sexual, pornografia e pedofilia entre outros);

IV. Que defendam ou incentivem atividades ilegais;

V. Que propaguem ou incentivem preconceito ou discriminação (assuntos de cunho religiosos, racial, sexual ou apologia a qualquer atividade ilegal ou ofensiva);

VI. Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da Corretora;

VII. Que possibilitem a cópia e/ou distribuição de informações de nível Interno e/ou Confidencial;

VIII. Que permitam a transferência (downloads e/ou uploads) de arquivos e/ou programas ilegais;

IX. Propagandas políticas;

X. Sites de mensagerias instantâneas e VoIP (Google talk, Hangouts, Whats app, Telegram, não limitado a estes), excetos aqueles permitido e autorizados pela Corretora;

XI. Rede sociais ou de relacionamento, exceto para áreas que necessitam deste acesso para executarem suas atividades; e

XII. Uso de *Anonymizer.*

O acesso à internet, para fins pessoais, é aceitável se usado com moderação e quando:

I. Não contrariar a legislação vigente, Documentos Corporativos e/ou as normas aqui descritas;

II. Não comprometer o desempenho dos sistemas da Corretora;

III. Não comprometer o desempenho do Colaborador Interno nas atividades do negócio da empresa;

IV. Não for utilizado para ganho ou lucro pessoal em atividades paralelas; e

V. Não interferir, negativamente, nas atividades profissionais, na empresa e em sua imagem.

14 Cópias de segurança

I. Manter seus dados e informações armazenados na rede da Corretora – *sharepoint / one drive* corporativo, pois os dados e informações salvos no disco local não possuem cópias de segurança (*Backup)*.

15 Descarte de dados

I. O descarte de informações ou ativos, deve ser feito de forma segura, com utilização de equipamentos apropriados;

II. O descarte impresso com dados internos ou confidenciais deve ocorrer após o seu uso utilizando o triturador do papel; e

III. Os equipamentos de TI que forem descartados, que contenham discos rígidos ou removíveis, deverão ter suas mídias destruídas pelo processo "*wipe*" de modo a não permitir a recuperação dos dados contidos.

16 Acesso

A Corretora conta com procedimentos e rotinas para a confirmação da identidade de todos os usuários de sistemas, equipamentos e entrada (portas);

16.1 Lógico

I. Manter controle do acesso aos dados e sistemas de modo a garantir que apenas pessoas autorizadas tenham acesso;

II. É vedada a cópia de dados ou informações para mídias de armazenamento externo que não estejam previstas nos Documentos Corporativos internos, exceto mediante autorização prévia da área de Compliance e de TSI;

III. Utilizar autenticação de dois fatores para os casos aplicáveis;

IV. O acesso ao ambiente tecnológico deve ser realizado através de login e senha; e

V. A conta do Colaborador será válida por tempo determinado, enquanto vigorar o contrato de trabalho ou do prestador de serviço.

É expressamente proibido aos usuários:

I. Compartilhar ou revelar suas credenciais de acesso a terceiros; e

II. Adotar em qualquer recurso de TI da instituição credenciais de acesso que venham a utilizar fora da instituição, para quaisquer fins.

16.2 Físico

I. Manter e registrar o controle do acesso as portas físicas de entrada de modo a garantir que apenas pessoas autorizadas tenham acesso;

II. Proteger o ambiente de negócio (operação) e processamento de tecnologia através de credencial de acesso; e

III. Manter restrito, com controles físicos apropriados e proporcionais à criticidade dos equipamentos, o acesso a todas as áreas onde serão processadas ou armazenadas informações pertinentes à operação da Corretora.

17 Papéis e responsabilidades

Compete a área de SI:

I. Garantir a implementação dos requisitos descritos neste tópico de Uso Aceitável, tal como; monitorar práticas não permitidas;

II. Comunicar ao gestor imediato do Colaborador Interno quanto ao não cumprimento das regras desta Política, por meio da identificação de alguma ação não permitida; e

III. Aprovar os acessos de exceção, quando estiver em acordo com o negócio do Grupo Ideal.

Compete ao colaborador:

I. É dever do usuário a proteção de suas credenciais de acesso à rede corporativa das empresas do Grupo Ideal. O compartilhamento de senha é proibido e o detentor da credencial de acesso assume a responsabilidade pela guarda, descrição ou sigilo das operações decorrentes do seu uso, responsabilizando-se pela utilização indevida.

Compete a área de TI:

I. Garantir a correta configuração dos mecanismos que possibilitam a utilização da Internet;

II. Liberar os sites aprovados pela área de Si;

III. Bloquear o acesso de todos os Colaboradores Internos a sites que se enquadrem nas categorias não permitidas;

IV. Avaliar a implementação dos requisitos descritos nesta Política;

V. Monitorar práticas não permitidas;

VI. Empreender os meios necessários para a prevenção da perda de dados através das ferramentas disponibilizadas, controlando o fluxo da informação, dados e arquivos que trafeguem pela rede;

VII. Comunicar ao gestor imediato do Colaborador Interno quanto ao não cumprimento das normas desta Política, por meio da identificação de alguma ação não permitida;

VIII. Manter atualizada uma lista de softwares homologados para utilização nos ambientes da Corretora;

IX. Estabelecer controle para a instalação de softwares.

X. Aplicar os requisitos descritos neste tópico de Uso Aceitável, através da correta configuração dos mecanismos de envio e recebimento de mensagens eletrônicas; e

XI. Comprometer-se em disponibilizar os mecanismos de envio e recebimento de mensagens eletrônicas.

18 Objetivo – Manual de identificação de usuários

Este tópico referente a Identificação de usuários tem como objetivo estabelecer um padrão para a confirmação da identidade dos usuários dos sistemas utilizados pela Corretora e regras para criação de senhas fortes e proteger e sustentar a troca de senha dos Colaboradores de forma segura.

19 Diretrizes

As seguintes diretrizes deverão ser seguidas:

I. Anteriormente a atribuição de usuários aos sistemas e dispositivos, a identidade do Colaborador Interno, prestador de serviço ou cliente deve ser confirmada;

II. A senha deve ser única, pessoal e intrasferível;

III. O usuário é o único responsável pelo uso de suas credenciais de acesso e o único responsável por qualquer transação efetuada durante o seu uso;

IV. Manter em sigilo total suas credenciais;

V. Referidas senhas deverão satisfazer os seguintes critérios de complexidade:

- Não conter partes significativas do nome da conta do usuário ou o nome todo;
- Conter no mínimo seis caracteres;
- Expirar em até 90 dias (exceto para usuários de sistemas e/ou serviços);
- Bloquear após 5 tentativas sem sucesso;
- Em caso de bloqueio da senha, o desbloqueio deverá ser feito manualmente pelo Administrador do sistema;
- Não repetir as últimas 6 senhas utilizadas;
- Armazenar as senhas de forma criptografada;
- Trocar obrigatoriamente a senha inicial quando esta for definida pelo administrador do sistema; e
- Conter caracteres de três das quatro categorias a seguir: caracteres maiúsculos (A-Z), caracteres minúsculos (a-z), números (0-9) e caracteres especiais (ex.: !, $, #, %).

VI. Utilizar dois fatores de autenticação, quando possível ou aplicável;

VII. As senhas devem ser criptografadas; e

VIII. Nunca armazenar ou gravar senha online ou no navegador de internet.

Proibido:

I. Guardar ou anotar a senha em local não aprovado para tal uso (ex.: papel, planilhas, documentos e texto etc.);

II. Compartilhar senhas com outros usuários;

III. Trafegar ou inserir senha em mensagens de e-mail, chamados, aplicativos de mensagens instantâneas ou outra forma de comunicação eletrônica; e

IV. Inserir senha abertas em arquivos de configuração de sistemas e dispositivos.

19.1 Usuários especiais

Os usuários com acessos especiais (Usuário administrador, privilegiado, serviço, banco de dados, sistemas, root etc.):

I. Devem trocar as senhas no primeiro acesso;
II. Configurar as senhas para não expirar;
III. Não podem introduzir senhas em arquivos ou script de forma aberta, sem criptografia; e
IV. Devem armazenar ou guardar as senhas em cofre de senha aprovados pela área de TI e TSI.

20 Papéis e responsabilidades

Compete à área de TI:

I. Manter a configuração de complexidade de senhas ativas nos sistemas e rede do ambiente tecnológico da Corretora; e
II. Bloquear e disponibilizar nova senha em caso de extravio, roubo ou perda da senha do Colaborador Interno, após comunicação mediante comprovação da identidade do usuário.

Compete ao Colaborador

I. Zelar pela sua senha;
II. Não compartilhar seu usuário e senha com terceiros; e
III. Comunicar a possibilidade de extravio, roubo ou furto de suas senhas ao time de SI.

21 Recomendação de proteção de senha

I. Não utilizar a mesma senha dos sistemas da Corretora em contas particulares e vice e versa;
II. Quando possível não utilizar a mesma senha de acesso de um sistema para mais de um sistema, tente utilizar senha diferente para sistema web, por exemplo;
III. Não revele sua senha por telefone, e-mail para NINGUEM, inclusive para seu superior direto ou diretoria;
IV. Não revele ou compartilhe sua senha mesmo enquanto estiver de férias ou ausente por qualquer motivo;
V. Não utilize o recurso “Lembrar senha” dos aplicativos, por exemplo em navegadores, rede social entre outros; e
VI. Sempre que possível utilize Cofre de senha para gerenciar e armazenar sua senha com segurança.