Manual de Segurança da Informação

Versão Consolidada: 3.0

Data da Aprovação: 13/02/2023

Aprovado por: Diretoria

TP ICAP Classification: Internal

ÍNDICE

Classification: Internal

1. Introdução

O objetivo da Segurança da Informação é manter o nível de segurança da organização em um patamar definido como adequado pela mesma e garantir que as diretrizes explicitadas neste Manual sejam praticadas. Isto é realizado através da implementação de controles que visam garantir a confidencialidade, a integridade e a disponibilidade das informações.

Para atingir este objetivo, a **Tullett Prebon Brasil CVC Ltda. ("TULLETT")** e a **ICAP do Brasil CTVM Ltda. ("ICAP")** estabelecem o presente Manual como um dos pilares de sua estratégia de segurança, que deve ser seguida e implementada para garantir que os ativos sejam protegidos de acordo com a sua importância estratégica para a organização.

O Manual de Segurança da Informação se define como um documento que expressa a posição das organizações sobre a segurança, quais são seus valores e direcionamentos para minimizar os riscos sobre seus ativos. Desta forma ela estabelece a linha mestra de atuação **da TULLETT e da ICAP**.em relação a todos os aspectos da segurança da informação, incluindo equipamentos, bens, informações e pessoas.

O Manual de Segurança da Informação tem como princípios assegurar a:

- Identificação: Garantir que qualquer indivíduo seja identificado unívoco e inequivocamente.
- Autenticação: garantir que a identidade das pessoas ou recurso seja expressamente comprovada.
- Autorização: garantir que somente as pessoas e recursos permitidos tenham acesso aos ativos.
- Confidencialidade: garantir que as informações sejam acessadas apenas por aqueles expressamente autorizados.
- Integridade: preservar a integridade das pessoas e ativos, salvaguardando-os contra ações não autorizadas e garantindo que todas as informações estejam exatas e completas durante a sua criação, uso, guarda e destruição.
- Disponibilidade: garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

Classification: Internal
TP ICAP Classification: Internal

Este documento serve como um guia de melhores práticas definida pelas Corretoras em relação à Segurança da Informação, e tem o propósito de oferecer uma base comum de atuação para ser usado por aqueles que são responsáveis pela criação, implementação e manutenção de processos, procedimentos, sistemas, tecnologias, conhecimento, estratégias, serviços, campanhas e quaisquer outros ativos que compõe o dia-a-dia da **TULLETT e ICAP** . As Empresas tem como compromisso assegurar que as orientações definidas neste documento sejam seguidas por toda a organização.

Este Manual deve ser revisado e atualizado periodicamente no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Após leitura, cada colaborador deve atestar que se compromete a respeitar e seguir as regras descritas neste Manual.

Antes de efetuar ações que envolvam acesso, uso, alteração, armazenamento, transmissão, destruição ou qualquer outra atividade envolvendo ativos da empresa, o usuário deve consultar este Manual para certificar-se de que a atividade é permitida. Toda e qualquer atividade que não seja claramente permitida é proibida. Em caso de dúvida o usuário deverá consultar seu Superior e/ou a Gerência de Tecnologia da Informação para assegurar-se que a atividade é permitida. Cabe a Gerência de Tecnologia avaliar os riscos das atividades não previstas nas diretrizes de segurança da empresa, levando ao conhecimento do Comitê Executivo a prática de alguma dessas atividades. O referido Comitê irá, em última instância, emitir parecer para resolução do mesmo.

2. Definições

Para o perfeito entendimento deste Manual, faz-se necessário definir o significado de alguns termos mencionados, são eles:

- Ativos: todo e qualquer bem material pertencente ou administrado pela Corretora, que podem ser:

    (i). Ativos de informação: base de dados e arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas, etc.

Classification: Internal
Classification: Internal

(ii). Ativos de *software*: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

(iii). Ativos físicos: equipamentos computacionais (computadores, processadores, monitores, *laptops*, *modems* etc.), equipamentos de comunicação (roteadores, PABX, telefones fixos ou celulares etc.), mídias (Pen-Drive, HD Externo, Fitas de Backup, discos ópticos etc.), outros equipamentos técnicos (no-breaks, aparelhos de ar-condicionado etc.), mobília, acomodações, etc.

- Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

- Assinatura Eletrônica: Informação que autentica uma mensagem.

- Antivírus: Programa que detecta e elimina vírus de computador.

- *Backup*: Cópia exata de um programa, disco ou arquivo de dados feitos para fins de arquivamento ou para salvaguardar informações.

- Cavalo de Tróia: Programa que pode danificar áreas da máquina e torná-la vulnerável ao ataque de hackers.

- *Chain letters*: e-mails enviados sucessivamente para diversas pessoas (correntes).

- Controle de Acesso: São restrições ao acesso às informações de um sistema exercido pela Gerência de Tecnologia da Informação.

- Criptografia: A arte e a ciência de utilizar matemática para tornar a informação segura e criar um grande nível de confiança no meio eletrônico.

- Direito de Acesso: É o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

- *Download*: É a transferência de um arquivo de um computador remoto para outro computador através da rede.

Classification: Internal

- Ferramentas: É um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades.

- *Firewall*: Dispositivo que controla o tráfego entre redes, sendo uma barreira entre elas.

- *Hacker:* Pessoa com conhecimentos técnicos sofisticados que a torna capaz de invadir sistemas de computadores.

- *Handheld:* Computadores ou dispositivos móveis que têm recursos para organização de documento pessoal e comunicação móvel.

- Incidente de Segurança: É qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo.

- *Junk mail:* São e-mails não solicitados por usuários não interessados em recebê-los.

- *Log:* Registro das transações ou atividades realizadas em um sistema de computador.

- *No-Break:* Sistema com baterias, que mantém o computador funcionando por um determinado período.

- *Peer-to-Peer:* Redes onde clientes compartilham entre si seus recursos bem como podem prover conteúdo e serviços à rede.

- Manual de Segurança: É um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação.

- Proteção dos Ativos: É o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém.

Classification: Internal

- Redes *Wireless:* Um tipo de rede que utiliza onda de rádio de alta frequência no lugar de cabos para fazer a comunicações entre as máquinas.

- Responsabilidade: É definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações.

- Senha de *Hardware:* Senha que não permite acesso ao computador. É configurada na BIOS.

- Senha Fraca ou Óbvia: É aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras com significado, dentre outras.

- *Spam:* E-mails não solicitados enviados para um grande número de pessoas, os quais fazem propaganda de produtos e serviços.

- Vírus: Programa construído para causar danos aos softwares do computador.

- Vulnerabilidade: Pode ser entendida como uma fragilidade inerente a um ativo de informação que, uma vez explorada ou aliada a uma ameaça, possa causar incidentes de segurança ou trazer prejuízo para a integridade do sistema. As vulnerabilidades podem ser de inúmeros tipos: humanas, técnicas, físicas, de mídia, de comunicação, etc.

- Webmail: Ferramenta web que permite acesso a caixa de e-mail corporativa através da internet.

3. Estrutura Normativa

A base da documentação de controles de segurança é o Manual de Segurança da Informação sendo complementada por outras Políticas Internas, que possuem o intuito de estabelecer de maneira mais detalhada quais proteções devem ser adotadas em casos específicos.

O Manual de Segurança da Informação prevê a publicação das seguintes outras Políticas a ela relacionadas:

Classification: Internal

- Política de Segurança da Informação para o Controle de Acesso Físico e Lógico.
- Políticas de Gestão de Mudanças e de Operações.
- Política de Segurança da Informação para o Uso de Portáteis.
- Política de Segurança da Informação para o Uso de Telefones.
- Política de Desenvolvimento de Sistemas Internos;

4. Abrangência

Este Manual se aplica às pessoas e ativos descritos abaixo:

Colaboradores

Todas as pessoas que, de alguma forma, prestem serviços para as Corretoras sejam elas: empregados, estagiários e terceiros (contratados, consultores, temporários ou outras denominações). Todos devem dar cumprimento às regras internas definidas neste Manual.

Ativos

Este Manual se aplica a todo equipamento, instalação, sistema e informações, bem como a quaisquer outros bens, tangíveis ou intangíveis, de propriedade ou administrados pela empresa.

Da mesma forma, se aplica a todas as plataformas de hardware e todos os sistemas operacionais e aplicativos utilizados. Aplica-se também a qualquer meio onde a informação possa ser armazenada, incluindo mídias magnéticas, discos ópticos, informações impressas em papel e material de marketing.

5. Privacidade

Informações pessoais e/ ou particulares, não devem ser colocadas ou deixadas em lugar algum do local de trabalho, tais como mesas, estantes, armários, sistemas de informática, sistemas telefônicos ou escritórios. A Administração tem o direito de acesso a qualquer dessas áreas e a todo o mobiliário. Os colaboradores não podem ter acesso à estação de trabalho de outro colaborador, inclusive arquivos eletrônicos, sem a prévia autorização da Gerência de Tecnologia e do *Compliance*.

Classification: Internal

6. Deveres e Responsabilidades

Todos os associados da **TULLETT e da ICAP** têm funções e responsabilidades relacionadas à segurança da informação. Estas funções e responsabilidades variam de acordo com a linha de negócios do colaborador e função dentro das Corretoras. As seguintes categorias de associados foram identificadas como tendo funções e responsabilidades diretas pelos controles de segurança da informação (para maiores informações sobre Funções e Responsabilidade, vide a Estrutura Organizacional das Corretoras).

6.1 Administração

É o Departamento responsável pela execução das atividades de custódia e/ou administração dos meios de informação não informatizados das Corretoras, tais como: fax, copiadoras, telefonia, controle de acesso físico, limpeza, arquivo, correio, mensageiros, impressoras, cabeamento, fragmentadores, salas de reunião e outros.

As responsabilidades específicas da Administração devem ser definidas e distribuídas pelas funções existentes para cuidar de cada meio de informação, isto é, cabe ao responsável pela Administração distribuir as funções específicas de segurança dos ativos de informação aos integrantes de seu Departamento.

Algumas das responsabilidades de segurança da informação são:

- Classificar os meios de informação não computadorizados que administra quanto à criticidade que representam, provendo as condições mínimas necessárias de continuidade, disponibilidade, integridade e legalidade desses meios, incluindo locais, serviços e equipamentos.
- Executar as ações para proteger os ativos de informação sob sua responsabilidade.
- Administrar os serviços de proteção, limpeza, transporte, armazenamento e destruição dos ativos de informação assegurando o cumprimento das condições definidas para a classificação que o ativo recebeu.
- Informar ao *Compliance* situações onde haja vulnerabilidade quanto à proteção dos ativos de informação das Corretoras.
- Assessorar na criação, alteração e manutenção de novas políticas, normas, códigos ou regulamentos de segurança da informação, juntamente com *Compliance*.

Classification: Internal
Classification: Internal

- Participar, quando cabível, na apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de segurança da informação aos regulamentos internos e externos da **TULLETT e da ICAP**.

6.2 Controles Internos & Compliance

É o Departamento que tem como foco principal garantir o cumprimento das normas regulamentares e aderência dos processos internos, prevenindo e controlando os riscos envolvidos nas atividades das Corretoras.

Responde pela estrutura que tem como funções, elaborar juntamente com o Departamento de Tecnologia da Informação as definições de Segurança da Informação e agir, de acordo com este plano, quanto à implementação e coordenação das ações necessárias.

Suas principais responsabilidades, entre outras, são:

- Realizar as atividades de revisão de administração de acesso.
- Formular e propor a criação e/ou revisão das políticas, procedimentos e diretrizes relacionados à segurança da informação.
- Assegurar a implementação deste Manual e demais regulamentos relacionados à segurança dos ativos de informação junto aos Departamentos.
- Promover campanhas de conscientização e treinamentos referentes à segurança dos ativos de informação.
- Verificar a adequação do Plano de Continuidade de Negócios das Corretoras.
- Assegurar que processos adequados foram instituídos para administrar os direitos dos colaboradores no acesso aos recursos de tecnologia.
- Registrar eventuais violações a este Manual, bem como, as demais normas relativas à segurança da informação.
- Assegurar que existam processos adequados para a verificação dos registros de atividades ("*logs*") em todos os sistemas e recursos de tecnologia e dados.
- Entender as regulamentações de negócio existentes e traduzi-las em controles sobre as informações das Corretoras.

6.3 Jurídico

É o Departamento que detém o conhecimento sobre as regulamentações e leis aplicáveis ao negócio e interesses das Corretoras.

Classification: Internal

O Jurídico possui algumas responsabilidades pertinentes à proteção dos ativos de informação das Corretoras, são elas:

- Assessorar a Instituição na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os ativos de informação.
- Participar, quando cabível, na apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de segurança da informação aos regulamentos internos e externos das Corretoras.
- Garantir que os contratos celebrados com outras entidades e pessoas externas à **TULLETT** e à **ICAP** contenham uma cláusula que preserve a segurança das informações das Corretoras e a manutenção dos arquivos.

A existência das diretrizes estabelecidas com base neste Manual e a necessidade do cumprimento de suas premissas devem ser referenciadas nos contratos e acordos com os fornecedores, clientes e terceiros, bem como nas obrigações dos demais colaboradores das Corretoras, de forma que cada um saiba suas obrigações, direitos e deveres com a segurança das informações.

6.4 Recursos Humanos

É o Departamento que executa as atividades relacionadas à administração de pessoal, treinamentos, salários, benefícios, contratação, transferência e desligamento de colaboradores.

Recursos Humanos tem algumas responsabilidades pertinentes à proteção dos ativos de informação das Corretoras, são elas:

- Fornecer, à estrutura responsável pela Segurança da Informação e de Infraestrutura, tempestivas informações sobre movimentação de colaboradores na companhia (desligamento, contratação, transferência, etc.) para que os responsáveis promovam a criação, modificação ou cancelamento da permissão de acesso;
- Organizar, juntamente com o *Compliance*, treinamentos relacionados à segurança dos ativos de informação.
- Divulgar e providenciar adesão dos novos colaboradores, caso cabível, às normas, políticas, códigos e regulamentos internos, no ato da admissão.

Classification: Internal
Classification: Internal

- Realizar a checagem das informações pessoais e profissionais prestadas pelos colaboradores e informar a Gerência as situações de conflito de interesses ou anormalidades.
- Criar, em conjunto com o *Compliance* e o Jurídico, e manter em arquivo os termos de confidencialidade e responsabilidade com todos os colaboradores das Corretoras, alterando os contratos, acordos e descritivos de cargos necessários.

6.5 Risco

É o Departamento executor, entre outras, das atividades de gerenciamento do risco das Corretoras e dos clientes. O Risco possui algumas responsabilidades pertinentes à proteção dos ativos de informação das Corretoras, são elas:

- Manter atualizado o Plano de Continuidade de Negócios das Corretoras.
- Coordenar o acionamento das medidas de emergência para fins de adoção dos procedimentos de continuidade de negócios das Corretoras.
- Realizar Testes de Continuidade e Contigência periódicos, mantendo histórico dos resultados e planos de ação implatados.
- Realizar monitoramentos dos riscos relacionados à segurança da informação.

6.6 Tecnologia da Informação

É o Departamento que tem como principais responsabilidades, a saber:

- Estabelecer as regras de proteção dos ativos das Corretoras.
- Decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas, de acordo com o documento Punição das Violações do Manual de Segurança da Informação.
- Revisar frequentemente as regras de proteção estabelecidas.
- Restringir e controlar o acesso e privilégios de usuários remotos e externos.
- Manter atualizada a Estratégia de Contingência dos Negócios.
- Executar as regras de proteção estabelecidas pelo Manual de Segurança da Informação.
- Detectar, identificar, registrar e comunicar a Gerência sobre violações ou tentativas de acesso não autorizadas.
- Definir e aplicar, para cada usuário de TI, restrições de acesso à rede, como horário e dias autorizados, entre outras.

Classification: Internal

- Manter registros de atividades de usuários de TI (*logs*) por um período de tempo superior a 5 (cinco) anos ou por um período superior caso solicitado pelo regulador. Os registros devem conter hora e data das atividades, identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc.).
- Limitar o prazo de validade das contas de prestadores de serviço ao período da contratação.
- Solicitar e gerir, quando necessário, auditoria para verificação de acessos indevidos.
- Solicitar, quando julgar necessário, o bloqueio de chaves de acesso de usuários.
- Excluir as contas inativas.
- Fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle.
- Atender demandas das auditorias internas e externas no que tange aos procedimentos da Tecnologia da Informação.
- Não enviar relatórios internos (ex: relatório de *Pen test,* indicadores de risco) sem antes solicitar aprovação ao Gerente imediato e a equipe do Compliance.

7. Uso dos Recursos de Tecnologia

7.1 *E-mail* Corporativo

O uso do *e-mail* corporativo ("*e-mail*") na Empresa está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. Seguem as regras de uso do *e-mail* corporativo:

- O e-mail deve ser usado apenas para propósitos relacionados com o negócio (ex.: para comunica-se com clientes e distribuidores e para juntar informações comerciais úteis).
- O usuário é o único responsável pelo conteúdo das transmissões feitas através do *e-mail* a partir de sua senha ou conta.
- As mensagens de *e-mail* são confidenciais, somente podendo ser acessadas pelo remetente e seu destinatário. É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela.

Classification: Internal

- Não deverão ser abertos arquivos ou executados programas anexados aos e-mails sem antes verificá-los com um antivírus.
- Não deve ser utilizado *e-mail* para fins ilegais.
- Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através do serviço.
- Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual.
- Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis.
- O colaborador não deverá obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço.
- Não devem ser utilizados os serviços para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia", ou outro programa prejudicial.
- Não devem ser transmitidas mensagens não-solicitadas, conhecidas como *spam* ou *junk mail*, correntes, ou distribuição em massa de mensagens não-solicitadas.
- Mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por vários usuários.
- Sempre que se ausentar, o usuário deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal.
- É proibido aos administradores de rede ou *e-mail* ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte.
- O tamanho máximo das mensagens e o tipo de arquivo enviado e recebido é limitado pelo Departamento de Tecnologia em função da análise da demanda de cada Departamento.
- Não é permitida a utilização do Webmail. O acesso será liberado somente com autorização da área de Compliance.

7.2 Uso do Telefone e FAX

O telefone (fixo e móvel) deve ser usado apenas para propósitos relacionados com o negócio (ex.: para comunica-se com clientes e distribuidores e para juntar informações comerciais úteis).

O uso de telefone fora da empresa para discussão de assuntos confidenciais internos pode ser necessário, porém pode gerar exposição de segurança. Recomendamos que o colaborador certifique-se de que não está sendo ouvido por pessoas próximas.

Classification: Internal

Não deixe mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas.

Evite enviar documentos confidenciais através de FAX. Se for inevitável, certifique-se de que o número de telefone que irá recebê-lo está correto.

Não utilize FAX de terceiros para enviar ou receber documentos confidenciais.

7.3 Uso da Internet

Alguns *sites* (páginas da Internet) contêm ou distribuem material que não são apropriados a um ambiente de trabalho. Os colaboradores não devem acessar tais *sites*, ou distribuir ou obter material similar através da *Internet*. Os acessos a *sites* podem estar sendo monitorados a qualquer tempo.

- Não é permitido o uso de serviços de mensagens ou *Chat* (*WhatsApp, Facebook Messenger*, etc.) e nem a *Webmail* (*Hotmail, Gmail, Yahoo, UOL, AOL*, etc.) nos equipamentos de uso exclusivo das Corretoras. As exceções poderão ser concedidas mediante autorização do gestor responsável e da área de Compliance.

Não é permitido o uso de compartilhadores de informações como redes *Peer-to-Peer*, também conhecidas como redes P2P (*eDonkey, eMule, Redes Torrent*, etc) dentro da Empresa.

Não é permitido o *download* de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

Seguem exemplos de tipos de *sites* proibidos:

- *Sites* que contenham imagens pornográficas ou materiais relacionados.
- *Sites* que contenham atividades ilegais.
- *Sites* que contenham intolerância por outros.
- *Sites de redes sociais (existem exceções para alguns departamentos).*

Classification: Internal

7.4 Uso da Rede Corporativa

Para assegurar o backup dos dados, os arquivos relacionados às atividades profissionais dos colaboradores nas Corretoras devem ser salvos na rede corporativa (cada Departamento possui pasta na rede corporativa) e não na raiz do computador.

Os arquivos a serem transferidos entre os colaboradores das Corretoras devem ser salvos na unidade Publico (P:\). Esta pasta, assim como todos os recursos de tecnologia, somente deve ser utilizada para fins estritamente profissionais, sendo o conteúdo, semanalmente, excluído pelo Departamento de Tecnologia.

A disponibilização de dados aos colaboradores é feita pelo *Compliance* uma vez que o acesso a porta USB e as mídias removíveis são bloqueadas, salvo as hipóteses autorizadas pela Diretoria com o conhecimento do *Compliance*.

É proibida a utilização da rede corporativa para o armazenamento de arquivos de áudio, imagens ou vídeos, salvo as áreas e/ou funcionários autorizados pelo Compliance.

7.5 Senhas de Acesso

Todo colaborador é responsável por todos os atos executados com seu identificador (login), que é único e requer senha exclusiva para identificação/autenticação individual no acesso à Informação e aos recursos de tecnologia e deve assegurar a confidencialidade de sua senha de acesso – ela não pode ser compartilhada, sendo de uso pessoal, intransferível e deverá ser trocada no primeiro acesso.

A senha é o meio de validação de acessos a recursos e serviços, portanto representa a assinatura digital do colaborador. Sendo assim, recomenda-se que cada colaborador coloque em práticas cuidados básico na proteção deste recurso:

- Manter a confidencialidade.
- Não devem ser óbvias, nem derivadas de dados pessoais.
- Devem ter pelo menos 8 (oito) caracteres.
- Devem conter pelo menos 1 (um) caracter alfabético.
- Devem conter pelo menos 1 (um) caracter numérico;
- Devem conter pelo menos 1 (um) caractere especial (! @ # $ % & *).
- Não devem conter mais de 3 (três) caracteres consecutivos idênticos a senha anterior.

Classification: Internal
Classification: Internal

- Devem ser trocadas pelo menos a cada 90 dias.
- Devem ser diferentes das 10 últimas senhas utilizadas.

7.6 Proteção Contra Vírus e Ataques

O vírus de computador é um programa desenhado para causar perda ou alteração de dados do computador.

Todo equipamento deve ter um programa antivírus instalado, sendo os softwares antivírus atualizados diária, automática e obrigatoriamente.

O colaborador deve efetuar regularmente a busca por vírus em seu computador. Caso seja encontrado vírus, o mesmo deverá consultar a equipe de suporte técnico para obter orientações.

Caso o colaborador receba algum *e-mail* alertando sobre vírus, não deverá passá-lo a outras pessoas, pois a maioria desses alertas é falso. Permanecendo a dúvida, deverá entrar em contato com a equipe de suporte técnico para maiores explicações.

7.7 Aquisição de *Software* & Direitos Autorais

A maioria das informações e *softwares* que estão disponíveis em domínio público (incluindo a *Internet*) está protegida por leis de Propriedade Intelectual, portanto:

- Arquivos e *softwares* só podem ser baixados com prévia aprovação do Departamento de Tecnologia. Quando tal ação representar obrigação onerosa e formal à **TULLETT e à ICAP,** é obrigatória a aprovação da respectiva Diretoria Comercial e Jurídica.
- Não é permitido obter *softwares*, imagens, etc. (*download*) destas fontes para uso nas Corretoras a não ser que haja uma permissão explícita por parte do seu dono.
- Deve-se ler e compreender todas as restrições dos direitos autorais do *software*. Caso a empresa não possa cumprir com as condições estipuladas, não deve ser feito *download* e não deve utilizar o material.
- O colaborador deverá garantir que cumpre com os requerimentos ou limitações requeridos pelo *software* (por exemplo, não pode ser utilizado para fins comerciais, não cobrar de outros o uso do *software*, etc.).
- É proibido o uso de qualquer foto, imagem ou desenho que possua marca registrada de terceiros. Pode-se utilizar imagens originais do Sistema

Classification: Internal
Classification: Internal

Operacional ou imagens não relacionadas a Produtos, Empresas ou Pessoas. Imagens consideradas agressivas também não devem ser utilizadas.

7.8 *Backup* e Restauração de Sistemas

A importância dos *backups* na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis, caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

Cada usuário tem um diretório no servidor de arquivos. Todos os documentos que digam respeito ao negócio deverão ser salvos neste diretório.

O *backup* de dados pessoais nas estações de trabalho é de total responsabilidade do usuário.

O *backup* dos servidores é executado pela equipe de Tecnologia da Informação responsável pelo mesmo seguindo os procedimentos definidos pela área e respeitando os prazos de retenção dos reguladores.

7.9 Notificações de Incidentes de Segurança

Qualquer suspeita de que está havendo um incidente de segurança deverá ser informada a Gerência de Tecnologia. Nenhum colaborador deverá investigar por conta própria, ou tomar ações para se defender do ataque, a não ser que seja instruído desta forma pela Gerência de Tecnologia. A Gerência de Tecnologia está capacitada para conter as exposições, analisar os impactos das Corretoras e conduzir investigações, coletando evidencias para possíveis ações jurídicas. Os incidentes são acompanhados mensalmente no comitê de Risco e *Compliance*.

7.10 Monitoramento

Os Departamentos de Tecnologia da Informação e *Compliance* efetuarão monitoramento da adequação quanto ao nível de controle e cumprimento deste Manual.

Os funcionários declaram-se cientes de que a **TULLETT** e a **ICAP.** reservam-se o direito de monitorar quaisquer atividades por ele desenvolvidas, através de todos os meios disponibilizados, tais como, e-mail corporativo, telefone, Mensageria, com o

Classification: Internal

intuito de identificar atividades suspeitas ou em desconformidade com este Manual, Políticas Internas e legislações existentes.

7.11 Tela Limpa

Computadores, *notebooks* e *handhelds* devem estar protegidos por senha quando não estiverem sendo assistidos.

7.12 Mesa Limpa

A política de mesa limpa consiste em não deixar informações confidenciais ou bens da empresa sem a devida proteção, acessíveis a outras pessoas, quando o colaborador estiver fora do seu local de trabalho. Incluem-se nesta política: papéis, Pen-Drives, CDs ou quaisquer outros tipos de mídias removíveis.

Ao final do dia de trabalho, computadores portáteis deverão ser trancados em uma gaveta, armário ou levados com o responsável pelo mesmo.

Informações confidenciais, quando impressas, devem ser imediatamente retiradas da impressora e trituradas, quando cabível.

Não é permitida alimentação, bebida e fumo próximo aos equipamentos.

Ocorrerão inspeções periódicas de "mesa limpa" nas estações e ambientes de trabalho.

7.13 Lixo Limpo

As informações confidenciais não devem ser depositadas no lixo, sendo obrigatória a destruição destes arquivos.

Ao final do dia de trabalho, estas informações devem ser colocadas na caixa disponibilizada no salão para trituração.

Ocorrerão inspeções periódicas de "lixo limpo" nas dependências das Corretoras.

Classification: Internal

8. Proteção do Patrimônio

Integram o patrimônio físico e intelectual da empresa, seus imóveis, instalações, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos colaboradores, não podendo os mesmos serem utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, seja para que fim for.

Não poderão ser utilizados equipamentos ou outros recursos das Corretoras para fins particulares, salvo se previamente autorizados pelo Superior hierárquico imediato. Não podendo ser aprovado caso:

- Interferir no trabalho do colaborador.
- Interferir ou concorrer com o negócio da empresa.
- Fornecer informação sobre, ou lista de colaboradores a outros.
- Envolver solicitação comercial ou outra solicitação não apropriada ao negócio.
- Envolver custo adicional para a empresa.

9. Atualização das Políticas Corporativas

A atualização deste Manual e demais Políticas Corporativas é de responsabilidade do *Compliance* e deve prever a conformidade com as mudanças e inovações legais e institucionais, acompanhando as alterações estratégicas de negócio.

Periodicamente, as Corretoras poderão publicar Políticas adicionais e/ou atualização, conforme consideradas necessárias ou apropriadas, sendo as mesmas divulgadas pelo *Compliance*, através de correio eletrônico e/ou Intranet, independente de qualquer outra formalidade.

10. Disciplina

A violação a este Manual ou a outras Políticas e Procedimentos Internos dará ensejo à ação disciplinar, iniciada e conduzida pelo *Compliance*.

Quanto aos graus de penalidades aplicáveis estes serão estabelecidos pelas Diretorias da **TULLETT e da ICAP** em função da gravidade da ocorrência e em função da reincidência ou não no descumprimento, podendo culminar em rescisão do contrato.

Classification: Internal

11. Considerações Finais

Este documento é de uso interno somente, todavia, em alguns casos poderá ser disponibilizado a terceiros somente com a ciência e aprovação do *Compliance* e o envio, exclusivamente, em meio físico ou em formato.pdf (documento protegido).

12. Histórico de Versões

Data	Versão	Descrição
15/01/2019	1.0	Versão inicial
13/07/2021	2.0	Atualização do item 7.5
09/02/2023	3.0	Revisão – sem alteração

Classification: Internal