GESTÃO INTEGRADA DE RISCOS DE TI

POL-0401

DATA 09/12/2020

1 Objetivo

Esta Política destina-se a atender os requisitos da Resolução 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.

Também se destina a atender os requisitos da Resolução nº 4.658/2018 e Instrução CVM 505, conforme alterada pela Instrução CVM 612, que dispõem sobre a obrigatoriedade da elaboração da Política de segurança cibernética e sobre determinados requisitos e procedimentos relacionados, a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil e àquelas sujeitas ao âmbito regulatório da Comissão de Valores Mobiliários (CVM).

As práticas de segurança cibernética incluem a gestão integrada de dispositivos de computação conectados, infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade das informações transmitidas e/ou armazenadas no ambiente cibernético.

2 Abrangência

Os requisitos descritos na Resolução Nº 4.557 abrangem os seguintes aspectos de segurança da informação:

- Integridade, segurança e disponibilidade dos dados e dos sistemas de informação utilizados;
- Robustez e adequação às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse; e
- Existência de mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais.

Esta Política é aplicável aos Colaboradores e fornecedores da Corretora que tenham acesso ao ambiente tecnológico e à rede da Corretora, em especial aos Colaboradores e prestadores de serviços da área de tecnologia da informação (TI).

2.1 Atribuições e responsabilidades

A área de TI é responsável por definir, gerir e monitorar os documentos corporativos de gestão integrada de riscos de TI em especial, mas não se limitando àqueles que tratam de segurança da informação e segurança cibernética.

A Diretoria da Ideal atua ativamente no sentido de suportar a implantação, o desenvolvimento e a promoção da cultura de segurança cibernética e segurança da informação na Corretora.

2.2 Violações

- Compete à área TI administrar e efetuar a gestão das situações de inadimplência com as regras de segurança da informação e segurança cibernética estabelecidas nesta Política, escalando ao Compliance e à Diretoria, conforme aplicável;
- Compete ao gestor 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 no regramento da Corretora, além das penalidades legais aplicáveis.

3 Alçada de aprovação

- A Superintendência de Tecnologia da Informação é responsável pela elaboração, manutenção, revisão e implementação desta Política.
- Cabe a área de Compliance conjuntamente com TI a revisão das alterações a esta Política.
- Compete à Diretoria a aprovação desta Política e de suas versões revisadas.

4 Revisão da Política

A revisão desta Política será realizada anualmente, ou em menor periodicidade se assim requerido pela Diretoria ou pelas áreas de TI e/ou Compliance.

4.1 Histórico de revisão

Revisor	Data	Descrição
Fabio Farias	01/11/2018	Versão original
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.

5 Glossário

Termo	Descrição
At Rest	Dados e informações gravadas em algum dispositivo físico ou lógico.

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	Computação em nuvem (em inglês, cloud computing), é um termo coloquial para a disponibilidade sob demanda de recursos do sistema de computador, especialmente armazenamento de dados e capacidade de computação, sem o gerenciamento ativo direto do utilizador. O termo geralmente é usado para descrever centros de dados disponíveis para muitos utilizadores pela Internet. Nuvens em grande escala, predominantes hoje em dia, geralmente têm funções distribuídas em vários locais dos servidores centrais. Se a conexão com o utilizador for relativamente próxima, pode ser designado um servidor de borda.
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
Detecção de Intrusão	Processo de monitoramento e análise de logs/eventos que ocorrem em um ambiente de computadores ou em uma rede de dados, para que se possa realizar análises em busca de indícios de incidentes ilegais (intrusão), os quais podem ser classificados como ameaças;
Espaço Cibernético	Ciberespaço, é considerado como a metáfora que descreve o espaço não físico criado por redes de computador, notadamente a internet, onde as pessoas podem se comunicar de diferentes maneiras, como por meio de mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros meios;
Fatores de Autenticação	Métodos utilizados pelos usuários de um sistema para confirmação de sua identidade. Existem 3 tipos de fatores de autenticação: i) algo que o usuário sabe (senhas, frases); algo que o usuário possui (token, e-mail, cartão de senhas); e algo que o usuário é (biometria digital, mapeamento da íris);
IaaS	Infrastructure as a Service é a forma mais básica de computação em nuvem, em que recursos computacionais básicos são ofertados e está mais próximo do termo computação em núvem. Os principais serviços IaaS são computação, armazenamento e redes.
In Transit	Dados e informações trafegadas entre dois dispositivos; e
Incidente Relevante	Incidente de segurança cibernética que: - Afete a integridade da rede da corretora, impossibilitando ou deteriorando o seu acesso; - Afete a integridade dos dados causando sua perda, roubo ou causem alterações a seus valores originais; ou - Degrade ou impossibilite o acesso de clientes aos sistemas disponibilizados.
Informação pessoal identificável ou 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 ou jurídica, seja ela cliente, fornecedor ou colaborador. Exemplos são

	números de documentos (RG, CPF, CNPJ, Código CVM), números de contas correntes ou de negociação, endereços, e-mail, posições em custódia e outros.
Intrusão	Ações realizadas com intuito de comprometer a estrutura básica da segurança de informação de um sistema informatizado, afetando sua integridade, confidencialidade e disponibilidade;
PaaS	Platform as a Service é o serviço de computação em nuvem que provê uma plataforma de computação, usualmente sistemas de middleware como Banco de Dados e Filas.
SaaS	Software as a Service é o serviço de computação em nuvem no qual sistemas empresariais são fornecidos como um serviço, podem ser desde Sistemas de Chamados até ERP's de grande porte.
Segurança Cibernética	O conjunto de metodologias e rotinas voltadas a assegurar a existência e a continuidade da sociedade da informação doe país, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas;
Sistemas Críticos	Sistemas que tem sua função principal o suporte aos processos de negociação, custódia e liquidação ou que auxiliam estes sistemas.

6 Diretrizes

Em relação à segurança da informação e segurança cibernética, as seguintes diretrizes deverão ser observadas de forma contínua:

- Tratar de maneira ética e sigilosa, as informações de clientes, usuários, parceiros, fornecedores e Colaboradores;
- Tratar de maneira ética e sigilosa informações de caráter confidencial, pessoal, sensível e restritas à Corretora;
- Capacitar tecnicamente e conscientizar constantemente os Colaboradores da Corretora e fornecedores acerca do trato e manejo da informação;
- Melhorar de maneira continua os processos e os procedimentos com base nos mais altos padrões de segurança aplicada à tecnologia da informação;
- Disseminar esta Política a todos os envolvidos na operação da Corretora, sejam eles Colaboradores ou terceiros, conforme aplicável;
- Confirmar o entendimento desta Política por parte de todos os envolvidos no início de suas contratações e anualmente, ou todas as vezes que esta seja modificada, conforme necessário; e
- Investir continuamente em aprimoramentos de tecnologia que assegurem a perenidade das premissas de segurança de informação e segurança cibernética.

7 Acesso lógico

A Corretora conta com procedimentos e rotinas para a confirmação da identidade de todos os usuários de sistemas e equipamentos;

Referidas rotinas contemplam todos os sistemas operacionais, equipamentos e softwares, estejam eles dentro da rede da Corretora ou em ambiente dos prestadores de serviços terceirizados, contendo informações confidenciais. Referidos parâmetros estão aptos a:

- Manter controle do acesso aos dados e sistemas de modo a garantir que apenas pessoas autorizadas tenham acesso;
- 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 TI;
- Assegurar, no mínimo, a aprovação do responsável pela informação e o gestor do Colaborador no momento da solicitação de determinado acesso;
- Identificar a autenticidade do usuário através de login criado ou solicitado pelo time de suporte de Tecnologia da Informação;
- Confirmar a identidade do usuário através da utilização de senhas fortes;
- Utilizar autenticação de dois fatores para todos os sistemas que sejam acessíveis através da Internet;
- Liberar acesso lógico somente aos recursos e informações necessários e indispensáveis ao desempenho das atividades dos Colaboradores e em conformidade com os interesses da Corretora;
- Permitir acesso lógico aos clientes apenas aos seus próprios dados, através de confirmação de sua identidade;
- Bloquear ou desabilitar todo e qualquer serviço de rede não autorizado.
- Registrar as autorizações de acesso aos sistemas;
- Revisar obrigatoriamente todos os acessos de um Colaborador no caso de mudança de função;
- Identificar através de matriz de segregação de atividades, acessos considerados tóxicos que, se combinados, podem gerar conflitos de interesse e, caso o acesso seja necessário, documentar aprovação da área de Compliance;
- Definir claramente os responsáveis pelas aprovações de acesso;
- Revisar, ao menos anualmente, os acessos concedidos; e
- Na ocorrência do desligamento de Colaboradores, o seu acesso ao ambiente de informações da Corretora deverá ser bloqueado imediatamente.

7.1 Parâmetros de senha

O acesso ao ambiente tecnológico ocorrerá através de senhas de autenticação do usuário, que deverão ser pessoais e intransferíveis. Referidas senhas deverão satisfazer os seguintes requisitos de complexidade:

- Não conter partes significativas do nome da conta do usuário ou o nome todo;
- Ter pelo menos seis caracteres de comprimento;
- Expirar, no máximo, a cada 90 dias (exceto para usuários de sistemas);
- Serem bloqueadas após, no máximo, 5 tentativas sem sucesso;
- Desbloquear através de ação do administrador do sistema;
- Não repetir, ao menos, as últimas 6 senhas utilizadas;
- Armazenar as senhas de forma criptografada;
- Trocar obrigatoriamente a senha inicial;
- Conter caracteres de três das quatro categorias a seguir: caracteres maiúsculos (A-Z), caracteres minúsculos (a-z), números (0-9) e caracteres especiais (ex.: !, $, #, %).

7.2 Segundo fator de autenticação

O acesso à rede fora do ambiente da corretora ou através de equipamento pessoal deve ser feito utilizando dois fatores de autenticação, que podem ser tokens, cartão de senhas, senhas de uso único enviados por e-mail, entre outros.

7.3 Acesso remoto

O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço e necessita de segundo fator de autenticação para sua disponibilidade aos usuários.

8 Acesso físico

Manter restrito, implementando 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, mantendo lista de acesso a estes ambientes.

9 Uso de equipamentos

Os equipamentos disponibilizados pela Corretora são de uso exclusivo para atividades da empresa, é vedado sua utilização para atividades não relacionadas, sendo que é dever dos Colaboradores empreenderem todos os esforços pelo uso racional dos equipamentos colaborando com a extensão de sua vida útil.

As estações de trabalho deverão estar sempre bloqueadas quando não estiverem sendo utilizadas, o bloqueio deve ocorrer automaticamente após um determinado período de inativação, que deverá ser estabelecido pela área de TI.

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

Os equipamentos de propriedade da Corretora devem ser identificados e catalogados, de forma a permitirem sua rastreabilidade e localização e em caso de extravio, avaliar a necessidade de abertura de um incidente de segurança para casos possíveis de perda de dados.

9.1 Instalação e utilização de softwares

- Somente softwares homologados e autorizados pela área de TI poderão ser instalados e utilizados;
- Somente a área de TI está autorizada a testar e homologar novos softwares;
- É proibido o uso de softwares ilegais ou em não-conformidade com a licença de uso do software; e
- A área de TI deverá estabelecer controle para a instalação de softwares.

10 Catálogo de componentes de tecnologia

Componente de tecnologia é qualquer equipamento, link de dados, sistemas e softwares em geral que esteja instalado no ambiente produtivo da Corretora. Estes componentes deverão ser catalogados e registrados em sistema específico de modo a permitir sua identificação e capturar, no mínimo as seguintes características:

- Código de identificação do componente;
- Nome e descrição;
- Dono do sistema;
- Dono dos dados;
- Responsável técnico;
- Classificação de componente crítico;
- Classificação de dados;
- Classificação de componente responsável por Informação Pessoal Identificável;
- Data de disponibilização em produção;

11 Uso do correio eletrônico

É um instrumento de comunicação interna e externa cujo objetivo é o de viabilizar a execução das atividades e negócios da Corretora. Referidas mensagens, quando intercambiadas, devem prezar pelo profissionalismo e ser elaboradas e enviadas de forma a não comprometer a imagem e nem aos princípios éticos da Corretora.

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

A corretora deve empreender os meios necessários para a prevenção da perda de dados através das ferramentas disponibilizadas, controlando o fluxo da informação, dados e arquivos por meio de correio eletrônico.

12 Uso do software de mensagens instantâneas

O uso de softwares de mensagens instantâneas para comunicação de assuntos relacionados a empresa e suas atividades, sejam elas informações classificadas como somente interno ou confidencial, deve se dar através de softwares autorizados. A sua utilização deverá ser disponibilizada exclusivamente para a execução das atividades e negócios da Corretora.

Informações 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.

As mensagens devem ser escritas em linguagem profissional, não devendo comprometer a imagem e nem os princípios éticos da Corretora.

A Corretora deve 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 por estes softwares.

13 Uso da internet

- O acesso à Internet será autorizado para os usuários conforme a necessidade para o desempenho de suas atividades na Corretora;
- É vedada a instalação de programas provenientes da Internet nos computadores da Corretora, sem expressa anuência da área de TI;
- É vedada a visualização, transferência (downloads e/ou uploads), cópia ou qualquer outro tipo de acesso a sites:
    - De conteúdo adulto;
    - Que defendam ou incentivem atividades ilegais;
    - Que propaguem ou incentivem preconceito ou discriminação;
    - Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da Corretora;
    - Que possibilitem a cópia e/ou distribuição de informações de nível Interno e/ou Confidencial; e
    - Que permitam a transferência (downloads e/ou uploads) de arquivos e/ou programas ilegais;
- O acesso a redes sociais será autorizado, mediante aprovação de Compliance, exclusivamente para atividades relacionadas ao negócio da empresa.

14 Tratamento de dados

A coleta de dados de clientes deverá se basear nos seguintes princípios:

- **Finalidade**: no ato da coleta de dados, os propósitos devem ser legítimos e explícitos**;**
- **Adequação:** o tratamento dos dados precisa ser adequado às finalidades comunicadas ao titular;
- **Necessidade:** só devem ser coletados os dados necessários e pertinentes à finalidade da empresa;
- **Livre acesso:** a qualquer momento, o titular dos dados pode consultar ou alterar as informações fornecidas;
- **Qualidade:** os dados utilizados pela empresa precisam ser claros, atuais e exatos no momento do tratamento;
- **Transparência:** sempre que quiserem, os titulares têm direito a receber explicações transparentes sobre o tratamento dos dados fornecidos;
- **Segurança:** a Corretora fica responsável pela segurança dos dados armazenados, e será responsabilizada em caso de perda, vazamento e alterações ilegais;

- **Prevenção:** é obrigatoriedade de a Corretora adotar medidas preventivas em relação à integridade dos dados;
- **Não discriminação:** é proibido utilizar os dados para fins discriminatórios, não só dos dados sensíveis mais quaisquer informações pessoais ou sensíveis;
- **Prestação de contas:** em caso de fiscalização ou solicitação por parte do proprietário do dado, a Corretora tem o dever de comprovar a observância a todos esses princípios.

14.1 Classificação de dados

Conceder acesso aos dados com base no princípio do *'Need to Know'*, ou seja, somente será dado acesso à informação para a pessoa que tiver a necessidade de conhecer aquela informação;

Os dados serão classificados de forma a identificar seu nível de confidencialidade;

A classificação pode ser:

- Público: quando o conteúdo puder ser distribuído a qualquer pessoa interna ou externa e for de conhecimento geral;
- Interno: conteúdo produzido pela Ideal para conhecimento exclusivo de seus Colaboradores, como documentação de sistemas, treinamentos, políticas, informativos etc.; e
- Confidencial: conteúdo sensível e de acesso apenas as pessoas que devam conhecer seu conteúdo, como dados pessoais e sensíveis de funcionários, terceiros, fornecedores e clientes, operações, posições, e transações de clientes.

14.2 Informação Pessoal Identificável

Informação Pessoal Identificável (dado pessoal e sensível) é toda e qualquer informação que separada ou em conjunto pode levar a identificação da pessoa física ou jurídica, seja ela cliente, fornecedor ou colaborador. Exemplos são números de documentos (RG, CPF, CNPJ, Código CVM), números de contas correntes ou de negociação, endereços, e-mail, posições em custódia e outros.

Essas informações devem ser tratadas de forma sigilosa e com máximo grau de segurança, de forma a limitar o acesso somente a quem necessita (*Need to Know*) e sua guarda deve ser feita de forma criptografada.

É necessária a identificação e controle de acesso de todos os sistemas e diretórios de arquivos que contenham Informação Pessoal Identificável, de modo a permitir o correto tratamento destas informações.

14.2.1 Autorização expressa

A coleta de dados de clientes deve ter autorização expressa do proprietário da informação e deve ser clara, indicando quais dados estão sendo coletados e qual a sua finalidade.

14.2.2 Educação dos Colaboradores

A Corretora deve dispor de meios para a conscientização dos Colaboradores e terceiros sobre o tratamento de Informação Pessoal Identificável, melhores práticas e os impactos das leis e regulamentações vigentes.

15 Cópias de segurança

A Corretora deve estabelecer procedimentos de cópias de segurança de seus sistemas, bancos de dados, diretórios de arquivos e configurações de equipamentos e que compreendam as seguintes diretrizes:

- Copiar os dados diariamente para local físico diferente do local de sua origem;
- Manter cópias de segurança das informações utilizadas na operação da Corretora por prazo compatível com legislação vigente;
- Efetuar retenção das mídias virtuais de cópia de segurança de acordo com o tipo de informação armazenada em conformidade com a regulamentação e legislação aplicável;
- Testar a restauração das cópias de segurança ao menos a cada 90 dias por amostragem.
- Efetuar armazenamento de informações consideradas confidenciais de modo criptografado; e

- Definir a periodicidade das rotinas de *backup*.

15.1 Trilhas de auditoria

Sistemas e rede corporativa devem manter trilhas de auditoria onde constem, ao menos, data e horário da execução, login, logout dos usuários, o registro que foi alterado e as ações executadas (Inclusão, exclusão e alteração) nos sistemas utilizados na operação da Corretora.

15.2 Segurança no descarte de material impresso

Estará à disposição dos Colaboradores trituradores de papel ou equipamento similar, para o descarte de material sensível;

Todo material impresso com dados internos ou confidenciais deve ser descartado após o seu uso utilizando o triturador do papel; e

Os Colaboradores deverão ser informados periodicamente sobre os procedimentos de descarte de material impresso.

15.3 Segurança no descarte de mídias físicas e equipamentos de ti

Todos os equipamentos de TI que forem descartados, que contenham discos rígidos ou removíveis, deverão ter suas mídias destruídas de modo a não permitir a recuperação dos dados contidos; e

Os equipamentos deverão seguir padrões de descarte que evitem impacto ao meio ambiente.

16 Ambiente de certificação

Todas as alterações em sistemas de informação deverão ser homologadas pelos usuários antes de serem promovidas a produção;

As homologações deverão ocorrer em ambiente segregado do ambiente de produção; e

O ambiente de homologação não deverá conter dados de produção, exceto quando com anuência do dono do sistema e por tempo determinado, tal evento deve ser registrado no sistema de registro de chamados.

17 Continuidade do negócio

De sorte a assegurar a continuidade de seus negócios em caso de situações adversas que possam comprometer a estrutura ou disponibilidade de seu escritório ou seus centros de processamento de dados, a Corretora deve dispor de um plano com medidas de garantia à continuidade dos processos críticos da corretora, junto a sistemas responsáveis por esse processo, sistemas que dão suporte a ele e toda sua infraestrutura de hardware e software.

O plano elaborado deve ser testado, no mínimo, anualmente para validar sua efetividade e todas as suas etapas e resultados devem ser registrados e evidenciados, devendo ser guardados por, no mínimo, 5 anos.

Após a execução dos testes, um relatório deve ser encaminhado para a Diretoria, contendo um resumo dos resultados e apontamentos de melhorias se for o caso.

17.1. Resiliência e testes de estresse de plataformas de terceiros.

17.1.1. Monitoramento de volume das operações originadas em plataformas de terceiros conectadas ao OMS da Corretora – A Corretora realizará anualmente testes de estresse nas plataformas de terceiros de forma a avaliar a capacidade e resiliência de determinados sistemas em situações de demanda excessiva. A

metodologia e características de referidos testes estará descrita em Documentos Corporativos de TI e poderá considerar em seu escopo, conforme aplicável, os sistemas de monitoramento do próprio OMS da Corretora."

18 Segurança cibernética

Com o aumento das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, torna-se obrigação das empresas dispender atenção para a segurança cibernética a fim de verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

18.1 As ameaças cibernéticas

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições financeiras, permitindo agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços;

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições;

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas ou hackers individuais, organismos de Estado, terroristas, colaboradores, competidores etc.). Os principais motivos identificados são:

- Obter ganho financeiro;
- Roubar, manipular ou adulterar informações;
- Obter vantagens competitivas e informações confidenciais de empresas concorrentes;
- Fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança;
- Promover ideias políticas e/ou sociais;
- Praticar o terror e disseminar pânico e caos.

18.2 Objetivos da segurança cibernética

Em consonância com a resolução 4.658 e a instrução CVM 505 (conforme alterada pela ICVM 612), a Corretora estabelece como objetivo da Segurança Cibernética: "proteger o ambiente virtual, auxiliar na higidez tecnológica do mercado financeiro e de capitais os ativos da Corretora, de seus clientes e usuários".

A proteção do ambiente virtual está embasada em diretrizes que visam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

O método adotado para proteção do ambiente virtual baseia-se em prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

18.3 Diretrizes de segurança cibernética

- **Identificação e Autenticação** – a Corretora conta com mecanismos que garantem a autenticidade e rastreabilidade dos usuários na utilização dos recursos computacionais, de forma a tornar possível a identificação dos autores de qualquer ação que seja feita utilizando os sistemas informatizados e meios de comunicação;
- **Criptografia** – existência de mecanismos de segurança e privacidade que tornam determinada comunicação (textos, imagens, vídeos etc.) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem";
- **Prevenção e Detecção de Intrusão** – existência de tecnologias projetadas para monitorar toda atividade de entrada e saída de uma rede de dados, identificando quaisquer padrões suspeitos de tráfego que podem indicar uma tentativa de ataque;
- **Prevenção de vazamento de informações** – a Corretora adota estratégias e tecnologias alinhadas com os processos de negócio para o controle da informação na sua utilização, compartilhamento e tráfego;
- **Varreduras para detecção de vulnerabilidades** – a Corretora definiu estratégias e implementou tecnologias que analisam os elementos que, ao serem explorados por ameaças, afetam a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa;

- **Proteção contra softwares maliciosos** – a Corretora se utiliza de tecnologias e soluções que visam mitigar proteger os dispositivos tecnológicos contra software malicioso, vírus, trojans e malwares;
- **Mecanismos de rastreabilidade** – a Corretora dispõe de tecnologias e soluções para monitorar o tráfego de informações e os recursos de processamento, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da Segurança Cibernética;
- **Segmentação da rede** – a Corretora definiu estratégias tecnológicas que contribuem com a excelência do desempenho e segurança da rede fazendo a separação dos domínios de rede segundo nível de acesso dos dispositivos ali contidos;
- **Manutenção das cópias de segurança** – a Corretora conta com processo para efetuar a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso de perda dos dados originais;
- **Registro e análise de impacto de incidentes ocorridos** – a Corretora conta com processo apto a registrar e analisar a causa dos incidentes ocorridos na infraestrutura de tecnologia da informação, fornecendo soluções para evitar a recorrência destes, minimizando e/ou evitando o impacto dos incidentes;
- **Controles de acesso** – a Corretora conta com tecnologia e procedimentos que visam permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um usuário ou um processo); e
- **Disseminação da cultura de segurança cibernética** – a Corretora estabeleceu procedimentos internos, tais como esta Política, que visam disponibilizar aos seus Colaboradores e terceiros, conforme aplicável, Documentos Corporativos que descrevem situações de risco cibernético a serem verificados nos processos e serviços da Corretora.

18.4 Criptografia

A Corretora adota procedimentos e soluções que permitem:

- Criptografar toda e qualquer informação transmitida (*in transit*) entre o ambiente interno e externo classificada como sigilosa conforme padrões homologados;
- Criptografar informações que são alvo típico de criminosos, tais como senhas de contas bancárias, números de cartões de crédito, senhas de sistemas, entre outras;
- Mapear os ativos digitais considerados críticos pela Corretora;
- Todos os dados e documentos armazenados (*at rest*) devem ser criptografados;
- Execução de processo contínuo e periódico de auditoria que teste as regras criptográficas aplicadas, a fim de assegurar o perfeito funcionamento da tecnologia no ambiente.

18.4.1 Chaves de criptografia e certificados digitais

- Manter de forma segura, a guarda das chaves de criptografia para acesso aos recursos computacionais;
- Manter registro de todas as chaves de criptografia e Certificados Digitais existentes, informando o dono e o mantenedor; e
- Documentar processo de guarda, renovação, revogação e inutilização de certificados digitais.

18.5 Prevenção e detecção de intrusão

Estabelecimento de procedimentos e soluções que permitem:

- Monitorar e analisar o tráfego e as atividades da rede;
- Examinar o tráfego de rede em busca de ameaças que gerem padrões incomuns de fluxo de dados;
- Liberar o tráfego legítimo para o destino (terminal, servidor); e
- Bloquear todo e qualquer tráfego considerado nocivo.

18.6 Prevenção de vazamento de informações

A Corretora conta com soluções e tecnologias de "*Data Loss Prevention*" (DLP), que permitem:

- Monitorar de forma constante a transmissão de dados;
- Monitorar ou bloquear a saída de dados confidenciais da rede;

- Monitorar e/ou bloquear, se necessário for, a transferência de dados;
- Implementar critérios e cláusulas no âmbito dos contratos com os fornecedores que estabeleçam as regras a serem seguidas pelos fornecedores no âmbito da prestação de serviços de tecnologia da informação prestados a Corretora;
- Implementar Documentos Corporativos que disciplinam o uso de ferramentas de comunicação, como e-mails e redes sociais pessoais;
- Evitar que arquivos salvos nos servidores sejam gravados em hds móveis ou enviados por e-mail sem uma autorização prévia;
- Implementar procedimentos de descarte e destruição de equipamentos de tecnologia da informação (desktops, hds, servidores etc.);
- Efetuar testes e elaboração periódica de relatórios sobre atividades relacionadas com vulnerabilidade das informações; e
- Implementar ferramentas para uso seguro de dispositivos pessoais no acesso a dados, informações e sistemas.

18.7 Análise de vulnerabilidades

A Corretora conta com procedimentos que permitam o gerenciamento de vulnerabilidades que conta com, no mínimo ferramentas aptas a:

- Identificar possíveis vulnerabilidades na rede, como portas abertas indevidamente;
- Identificar possíveis vulnerabilidades conhecidas em versões de sistemas operacionais e softwares de infraestrutura (bancos de dados, Gerenciadores de Filas, Gerenciadores de Containers, firewalls etc.);
- Classificar por nível de impacto e criticidade as vulnerabilidades identificadas; e
- Definir plano de remediação das vulnerabilidades baseado em sua criticidade.

18.8 Testes de penetração de sistemas e rede

A Corretora conta com procedimentos de testes periódicos de penetração de sistemas e a parte de sua rede que são expostos a rede mundial de computadores. Estes procedimentos devem no mínimo:

- Definir a periodicidade dos testes que não deve ser maior que 1 (um) ano;
- Definir os responsáveis pela condução dos testes;
- Definir as ferramentas que serão utilizadas no processo;
- Definir como serão tratados os problemas encontrados durante a análise e os tempos de correção; e
- Definir quais níveis de problemas são aceitos para que um sistema entre em produção;

18.9 Proteção contra softwares maliciosos

A Corretora conta com procedimentos, soluções e tecnologias pertinentes à proteção contra softwares maliciosos, que permitem:

- Proteger servidores físicos e virtuais, estações, dispositivos móveis e dispositivos de segurança da informação contra softwares maliciosos;
- Atualizar periodicamente, conforme disponibilização de versão do fabricante, os produtos utilizados para proteção contra softwares maliciosos;
- Estabelecer procedimentos que visem os controles de detecção, prevenção e combate a softwares maliciosos;
- Verificar a presença de códigos maliciosos, antes de serem utilizados, em todos os arquivos recebidos por meio de redes, em qualquer mídia de armazenamento, correio eletrônico, arquivos baixados (download) ou em páginas web;
- Analisar os arquivos que estão sendo obtidos pela internet;
- Verificar continuamente as mídias de forma transparente ao usuário; e
- Emitir alertas sempre que um software malicioso for detectado.

18.10 Mecanismos de rastreabilidade da informação

A Corretora conta com procedimentos, tecnologias e soluções de rastreabilidade que permitem:

- Identificar todos os sistemas que contenham informações de clientes da Corretora;
- Garantir que os sistemas identificados possuam trilhas de auditoria;
- Garantir que as operações de entrada e saída de informações dos clientes estejam gravadas nas trilhas de auditoria;
- Garantir as trilhas de login e logout dos sistemas identificados; e
- Garantir a implantação de controles internos que permitam auditar a rastreabilidade das informações.

18.11 Segmentação da rede

A topologia de rede da Corretora deve ser capaz de:

- Efetuar a segmentação por sub-redes, de forma a segregar os dispositivos de diferentes níveis de acesso;
- Restringir o acesso não autorizado; e
- Efetuar o controle e a rastreabilidade das conexões.

18.12 Registro e análise de impacto de incidentes ocorridos

A Corretora conta com procedimentos pertinentes à implantação do registro dos incidentes que permitem:

- Efetuar o registro das informações pertinentes ao incidente ocorrido;
- Analisar o incidente e estabelecer plano de ação visando a sua solução;
- Através do registro das informações, gerenciar os incidentes garantindo que eles sejam solucionados o mais rápido possível;
- Manter por 5 (cinco) anos todos os registros de incidentes de segurança da informação;
- Comunicar ao mercado e aos reguladores tempestivamente a ocorrência de incidentes;
- Em caso de comprometimento de informações pessoais identificáveis, informar as pessoas impactadas;
- Através do registro das informações, reduzir o impacto dos incidentes nos níveis de serviço preestabelecidos entre fornecedor e cliente.

18.13 Disseminação da cultura de segurança da informação e cibernética

A Corretora adota procedimentos e métodos como forma de capacitação e de disseminação da segurança cibernética e da informação, a saber:

- **Cartilha de Segurança** - instrumento de comunicação disponibilizado a todos os Colaboradores descrevendo as situações de Segurança Cibernética que poderiam ser verificadas nas operações da Corretora;
- **Divulgação para clientes** – manter no site, de forma acessível para os clientes, informações referentes à Segurança Cibernética;
- **Monitoramento** – adoção de mecanismos que certificam a leitura, por parte dos Colaboradores da Cartilha de Segurança Cibernética bem como desta Política;
- **Campanhas e recertificação:** de ser feito rotineiramente, em períodos anuais, campanhas de conscientização e avaliação da efetividade da disseminação da cultura de segurança e identificação da necessidade de recertificação de colaboradores com base em avaliação do entendimento da dos conteúdos oferecidos;

18.14 Programa de Segurança Cibernética

Anualmente o time de Tecnologia da Informação deve apresentar ao comitê executivo, o programa de segurança cibernética que, entre outros pontos, deve endereçar:

- a identificação e avaliação dos riscos cibernéticos internos e externos a que a corretora esteja exposta;
- as medidas que devem ser adotadas para reduzir a vulnerabilidade da instituição contra ataques cibernéticos;

- procedimentos e controles internos que serão adotados para:
  - verificar a implementação, a aplicação e a eficácia das medidas; e
  - efetuar o monitoramento contínuo e a detecção de ataques cibernéticos em tempo hábil;
- medidas que serão adotadas para tratamento de incidentes cibernéticos e recuperação de dados e sistemas;
- periodicidade com que o programa de segurança cibernética será testado e revisado, de forma a:
  - avaliar a vulnerabilidade da corretora contra ataques cibernéticos e identificar novos riscos cibernéticos; e
  - verificar a necessidade de aperfeiçoar as regras, procedimentos e controles internos existentes;
- formas de participação em iniciativas que objetivem o compartilhamento de informações sobre ameaças e vulnerabilidades relevantes.

19 Critérios e Requisitos para a contratação de serviços de Computação em Nuvem

A contratação de serviços em nuvem deve levar em conta os seguintes critérios:

- Há alterativas à terceirização em si?

  Em havendo, ou seja, caso seja possível o desenvolvimento e a condução das atividades em questão internamente, devem-se considerar:

- Trata-se de atividade fim ou atividade meio? Em linhas gerais, atividades-fim, ou seja, os serviços entregues pela própria Corretora, não serão terceirizados.

- E, assumindo-se que a terceirização faça sentido econômico, ela pode diferenciar, de maneira sensível a experiencia dos cientes da Corretora? E/ou pode resultar em vantagem(ns) competitiva(s)

Naturalmente, o grau de complexidade da contratação deve ser examinado na avaliação dos critérios acima. Devem-se observar, em particular, as diretrizes no documento interno POL-0005 - Alterações ao Front-to-Back, que fornece os princípios e conceitos adotados pela Corretora na avaliação da abrangência (e complexidade) de eventuais alterações em sua infraestrutura corporativa (ou “Front-to-Back”), em que se incluiria a contratação de serviços em nuvem.

A contratação de serviços relevantes em nuvem, que suportem sistemas críticos e/ou Informações Pessoais Identificáveis ou Informações Sensíveis, deve levar em consideração os requisitos mínimos que a contratada deve atender durante a prestação dos serviços, que são:

- Segregação dos dados: a contratada deve garantir a segregação física e/ou lógica dos dados da corretora em relação a outros clientes da contratada;
- Controle de Acesso: o serviço deve permitir controle de acesso adequado que garanta a segregação de acesso entre diferentes funções da corretora;
- A contratada deve possuir processos e procedimentos que garantam a disponibilidade, integridade e confidencialidade das informações processadas e/ou armazenadas. A contratada também deve prover documentação suficiente para demonstrar que os processos e procedimentos estão adequados ou contar com auditoria externa independente que, neste caso, deve apresentar os relatórios de conclusão;
- A Contratada deve contar com monitoramento adequado às necessidades da Corretora e disponibilizar informações relevantes quanto à saúde dos serviços prestados em tempo real;
- A Contratada deve contar com procedimentos de testes de penetração e verificação de vulnerabilidades periódicos e o resumo dos relatórios devem ser disponibilizados à Corretora sempre que solicitado.

19.1 Contratação de serviços de PaaS e IaaS

Na contratação de serviços em nuvem no modelo PaaS (Platform as a Service) e IaaS (Infrastructure as a Service) é necessário observar alguns critérios adicionais:

- Criptografia: os dados da corretora devem ser mantidos e transferidos de forma criptografada e apenas o pessoal autorizado da Corretora deve ter acesso às chaves criptográficas que decifram os dados;
- O serviço deve disponibilizar redundância de datacenters na mesma região/país;
- O provedor de nuvem deve possuir as certificações válidas e auditadas de, ao menos: CSA (controles da Cloud Security Alliance), ISO9001, ISO27001, ISO27017, ISO27018, SOC1, SOC2 e SOC3

19.2 Cláusulas contratuais obrigatórias

Na contratação de serviços de nuvem que processem ou armazenem Informações Pessoais ou Sensíveis ou que atendam a sistemas críticos da corretora, as cláusulas contratuais devem dispor de:

- Localização onde os serviços poderão ser processados e/ou armazenados, indicando pais e região;
- Medidas de segurança dos dados processados e/ou armazenados;
- Segregação dos dados processados e/ou armazenados;
- Segregação dos controles de acesso;
- Prever a obrigatoriedade, em caso de extinção do contrato, de: i) transferência de todos os dados armazenados de volta à Corretora; e ii) a exclusão de todos os dados armazenados, incluindo códigos fontes, bancos de dados e arquivos de todos os gêneros, após confirmação do recebimento dos dados pela Corretora e da validação de sua integridade e disponibilidade;
- O acesso às informações relativas: i) às certificações e aos relatórios de auditoria especializada e; ii) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação de a empresa contratada notificar a corretora sobre a subcontratação de serviços relevantes para a instituição;
- A permissão de acesso do Banco Central do Brasil e, conforme aplicável ao serviço em questão, aos demais reguladores e autorreguladores com competência fiscalizatória sobre a Corretora, aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;
- A adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e
- A obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

19.2.1 O contrato deve prever ainda:

Para o caso da decretação de regime de resolução da Corretora pelo Banco Central do Brasil:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no item 19.2 dessa Política, que estejam em poder da empresa contratada; e
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:
    - a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução e;
    - a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.