

POLÍTICA DE SEGURANÇA CIBERNÉTICA

EXECUTIVE SOCIEDADE CORRETORA DE CâMBIO LTDA

Data Base 15/01/2020
Versão: 3º
Última Atualização: 01/06/2026

Sumário

1. OBJETIVO	4
2. RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS	4
3. RESPONSABILIDADES	6
4. DIRETRIZES	8
4.1 CLASSIFICAÇÃO DA INFORMAÇÃO	10
4.1.1. NÍVEIS DE CLASSIFICAÇÃO	10
4.1.2. CRITÉRIOS DE CLASSIFICAÇÃO	11
4.1.3. CONTROLES ASSOCIADOS À CLASSIFICAÇÃO E RESPONSABILIDADES	11
5. PLANO DE AÇÃO / RESPOSTAS A INCIDENTES	12
5.1. IMPLEMENTAÇÃO DA POLÍTICA	12
5.2. RELATÓRIO SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES	12
6. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM	13
6.1 EXIGÊNCIAS PARA A CONTRATAÇÃO DE SERVIÇOS	13
6.2 AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS	14
6.3. COMUNICAÇÕES AO BANCO CENTRAL	15
6.4. DOS CONTRATOS	16
7. PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO	17
7.1. MITIGAÇÃO DOS RISCOS E PROCEDIMENTOS DE CONTROLE	17
7.1.1. AUTENTICAÇÃO E GESTÃO DE IDENTIDADE	19
7.1.2. GESTÃO DE IDENTIDADE E ACESSO (IAM)	19
7.1.3. REGISTRO, MONITORAMENTO E RASTREABILIDADE	20
7.1.4. CONTROLES COMPLEMENTARES	21
7.1.5. SEGURANÇA NA INTEGRAÇÃO DE SISTEMAS (APIs)	21
7.1.5.1. REGISTRO, MONITORAMENTO E RASTREABILIDADE	21
7.1.6. CULTURA DE SEGURANÇA	23
7.2. PROTEÇÃO DE DADOS	24
7.3. AÇÕES DE PREVENÇÃO	32
7.3.1. GESTÃO DE VULNERABILIDADES	32
7.3.2. IDENTIFICAÇÃO DE VULNERABILIDADES	33

7.3.3. AVALIAÇÃO E CLASSIFICAÇÃO DE RISCOS	33
7.3.3.1. METODOLOGIA DE CLASSIFICAÇÃO DE RISCOS CIBERNÉTICOS	33
7.3.4. TRATAMENTO E REMEDIAÇÃO	34
7.3.5. REGISTRO, MONITORAMENTO E GOVERNANÇA	35
7.3.5.1. INTEGRAÇÃO COM GESTÃO DE RISCOS	35
7.3.6. REGISTROS E RASTREABILIDADE	36
7.4. TRATAMENTO DE INCIDENTES	36
7.5 INTELIGÊNCIA EM CIBERSEGURANÇA	39
7.6. MONITORAMENTO E TESTES	41
8. CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES	42
9. MONITORAMENTO, INDICADORES E REPORTE DE SEGURANÇA CIBERNÉTICA ..	42
10. DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL	44
11. REGULAMENTAÇÃO ASSOCIADA	44
12. ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA	45

1. OBJETIVO

Este normativo estabelece a Política de Segurança Cibernética da Executive Corretora de Câmbio, bem como os requisitos para a Contratação, Avaliação e Gestão de serviços de processamento e armazenamento de dados e de computação em nuvem visando total observância e adequação ao exigido na RESOLUÇÃO CMN Nº 4.893, DE 26 DE FEVEREIRO DE 2021.

O principal objetivo desta Política é assegurar a proteção dos ativos de informação da Corretora contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo de nossos negócios.

2. RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das Instituições Financeiras, permitindo assim 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, hackers individuais, terroristas, colaboradores, competidores etc.) como por exemplo:

- **Ganhos financeiros através de roubo, manipulação ou adulteração de informações;**
- **Obter vantagens competitivas e informações confidenciais de clientes ou instituições concorrentes;**
- **Fraudar, sabotar ou expor a instituição invadida por motivos de vingança, ideias políticas ou sociais;**
- **Praticar o terror e disseminar pânico e caos;**
- **Enfrentar desafios e/ou ter adoração por hackers famosos.**

Os invasores podem utilizar vários métodos para os ataques cibernéticos, destacam-se os mais comuns:

- **Malware:** softwares desenvolvidos para corromper computadores e redes;
- **Vírus:** software que causa danos a máquina, rede, softwares e banco de dados;
- **Cavalo de Troia:** aparece dentro de outro software e cria uma porta para a invasão do computador;
- **Spyware:** software malicioso para coletar e monitorar o uso de informações;
- **Ransomware:** software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- **Engenharia social:** métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito;
- **Pharming:** direciona o usuário para um site fraudulento, sem o seu conhecimento;
- **Phishing:** links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- **Vishing:** simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- **Smishing:** simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- **Acesso pessoal:** pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- **Ataques de DDOS (*Distributed denial of services*) e botnets:** ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- **Invasões (*advanced persistent threats*)** – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização. As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial,

além de riscos operacionais. Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.

Tanto instituições grandes como pequenas podem ser impactadas e por esse motivo os ativos incorporados no espaço cibernético devem ser protegidos e preservados sendo também essa necessidade um dos motivos da implementação desta Política.

Entre esses ativos cibernéticos estão:

- Softwares, como um programa de computador;
- Conectividades como acesso à internet, Banco Central, Receita Federal etc.
- Informações sigilosas de clientes e da própria corretora
- Componentes físicos, como servidores, estações de trabalho, notebooks etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores de mercado, incluindo o Banco Central, têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

3. RESPONSABILIDADES

Responsável: Diretor responsável pela Política de Segurança Cibernética

Atribuições:

- Responsável pela Política de Segurança Cibernética;
- Responsável pela execução do Plano de Ação e de resposta a incidentes.

O Diretor responsável pela Política de Segurança Cibernética pode desempenhar outras funções na Corretora desde que não haja conflitos de interesses.

Atribuições dos Diretores e gestores de área:

- Zelar pelo cumprimento destas normas e procedimentos, notificar imediatamente ao TI qualquer vulnerabilidade e/ou ameaça de quebra de segurança;

- Solicitar acesso para os usuários, através do sistema de chamados, bem como atualizar as solicitações de autorização sempre que houver alterações nos sistemas ou funções nas áreas de atuação;
- Os usuários Administrador e de Sistemas Bancos de Dados, ficarão sob responsabilidade do Diretor designado para a Segurança Cibernética. O responsável por acesso, liberação ou sistema; quando afastado, poderá conceder temporariamente seus direitos de acesso ao seu substituto ou a um diretor, revogando assim que retornar;
- Advertir formalmente o usuário e aplicar as sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao TI;
- Comprometer-se com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

São atributos exclusivos do Departamento de Tecnologia e Informação – TI:

- Definir, executar e divulgar as medidas de Segurança da Informação;
- Instalar ou remover componentes, fazer manutenção e controlar hardware e software;
- Autorizar tecnicamente a aquisição de hardware e software;
- Realizar verificações e/ou auditorias de hardware e software, com a finalidade de garantir a proteção dos recursos computacionais;
- Adquirir serviços de informática.

Atribuições dos Usuários:

- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Adquirir conhecimento técnico necessário para a correta utilização dos recursos;
- Relatar prontamente ao Gestor do TI qualquer fato ou ameaça à segurança dos recursos tais como: Quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas e/ou diretórios de rede, acesso indevido à Internet, programas instalados sem conhecimento do TI, etc.;

- Não tentar obter acesso não autorizado a sistemas ou recursos de redes de computadores internas ou externas;
- Assegurar que as informações e dados de propriedade da INSTITUIÇÃO não sejam disponibilizados a terceiros, a não ser com prévia autorização da diretoria;
- Solicitar ao Gestor do TI a possibilidade de instalação de um novo software ou aquisição de novo Hardware para a melhoria dos serviços prestados.

4. DIRETRIZES

A Política de Segurança Cibernética, que está implementada na Executive Corretora de Câmbio baseia-se nos seguintes princípios:

- Assegurar a **confidencialidade** dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) observadas as regras de sigilo e confidencialidade vigentes.
- Assegurar a **integridade** (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- Assegurar a **disponibilidade** dos dados e sistemas de informação utilizados na Corretora (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário).

A implementação desta Política considera as seguintes compatibilidades da Corretora:

- O porte, perfil de risco e o modelo de nossos negócios;
- A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais.
- A sensibilidade dos dados e das informações sob responsabilidade da instituição.

Os ambientes, sistemas, computadores e redes da Corretora poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Caberá a todos os Colaboradores conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados,

assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercício de suas atividades.

A Política de Segurança Cibernética é orientada por princípios estratégicos, incluindo:

- a) Abordagem baseada em risco;
- b) Melhoria contínua dos controles;
- c) Proporcionalidade ao porte e complexidade;
- d) Resiliência operacional;
- e) Alinhamento com objetivos estratégicos da instituição.

A alta administração é responsável por assegurar que a segurança cibernética seja tratada como elemento estratégico do negócio.

Conforme a Resolução nº 4.893/21, os serviços de computação em nuvem abrangem a disponibilidade da Executive Corretora de Câmbio, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a Executive Corretora de Câmbio implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos.
- Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela Executive Corretora de Câmbio utilizando recursos computacionais de seus prestadores de serviços.
- Execução por meio de Internet dos aplicativos implantados ou desenvolvidos por prestadores de serviços da Executive Corretora de Câmbio, com utilização de recursos computacionais do próprio prestador de serviços contratado pela Corretora.

A Executive Corretora de Câmbio é responsável pela Gestão dos serviços contratados incluindo as seguintes atividades:

- Análises de informações e de recursos adequados ao monitoramento dos serviços.
- Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a Prestadores de serviços
- Cumprimento da legislação e da regulamentação vigente.

4.1 CLASSIFICAÇÃO DA INFORMAÇÃO

A Executive Corretora de Câmbio estabelece e mantém processo formal de classificação da informação, com o objetivo de assegurar o adequado nível de proteção das informações, considerando sua sensibilidade, criticidade e impacto potencial em caso de acesso, alteração, divulgação ou perda não autorizada.

A classificação deverá ser aplicada a todos os dados e informações sob responsabilidade da instituição, independentemente do meio de armazenamento, processamento ou transmissão.

4.1.1. NÍVEIS DE CLASSIFICAÇÃO

As informações são ser classificadas, no mínimo, nas seguintes categorias:

a) Pública: Informações que podem ser divulgadas ao público em geral, sem restrições, não acarretando riscos à instituição, clientes ou parceiros.

b) Interna: Informações de uso exclusivo da instituição, cujo acesso deve ser restrito a colaboradores e terceiros autorizados, podendo causar impactos operacionais ou administrativos em caso de divulgação indevida.

c) Confidencial: Informações sensíveis relacionadas às atividades da instituição, clientes, operações ou estratégias, cujo acesso deve ser rigorosamente controlado, podendo gerar impactos relevantes financeiros, regulatórios ou reputacionais em caso de exposição indevida.

d) Restrita: Informações altamente sensíveis e críticas, cujo acesso deve ser limitado a um grupo extremamente restrito de usuários autorizados, sendo sua divulgação, alteração ou destruição não autorizada capaz de causar impactos severos à instituição, clientes ou ao sistema financeiro.

A classificação das informações deverá ser revista periodicamente ou sempre que houver alteração relevante no contexto do negócio da a Executive Corretora de Câmbio, na sensibilidade dos dados ou nos requisitos regulatórios aplicáveis.

O processo de classificação da informação deverá ser formalmente documentado e mantido disponível para fins de auditoria, supervisão regulatória e melhoria contínua.

4.1.2. CRITÉRIOS DE CLASSIFICAÇÃO

A classificação da informação considera, no mínimo:

- a) Sensibilidade dos dados;
- b) Relevância para as operações da instituição;
- c) Impacto potencial em caso de violação de confidencialidade, integridade ou disponibilidade;
- d) Requisitos legais e regulatórios aplicáveis.

Assim, a Executive Corretora de Câmbio assegura que:

- a) As informações sejam claramente identificadas quanto ao seu nível de classificação, sempre que aplicável;
- b) Prestadores de serviços e terceiros observem os mesmos requisitos de classificação e proteção;
- c) A classificação da informação esteja integrada aos processos de gestão de acesso, segurança cibernética, continuidade de negócios e proteção de dados pessoais.

4.1.3. CONTROLES ASSOCIADOS À CLASSIFICAÇÃO E RESPONSABILIDADES

Para cada nível de classificação a Executive Corretora de Câmbio deverá possuir controles proporcionais, incluindo:

- a) Definição de perfis de acesso e restrições de uso;
- b) Requisitos de proteção no armazenamento, inclusive com uso de criptografia quando aplicável;
- c) Regras para transmissão e compartilhamento de informações;
- d) Procedimentos para descarte seguro de dados;
- e) Aplicação de mecanismos de monitoramento e rastreabilidade de acesso.

As responsabilidades referentes aos níveis de classificação, seguem as seguintes diretrizes e controles:

- a) Os responsáveis pelos processos e áreas deverão classificar as informações sob sua gestão, garantindo sua correta identificação e proteção;
- b) Os usuários deverão respeitar a classificação atribuída, utilizando as informações apenas para os fins autorizados;
- c) A área responsável por Segurança da Informação deverá orientar, monitorar e revisar periodicamente os critérios e práticas de classificação adotados.

5. PLANO DE AÇÃO / RESPOSTAS A INCIDENTES

5.1. IMPLEMENTAÇÃO DA POLÍTICA

Visando a implementação das práticas da Política de Segurança Cibernética na Executive Corretora de Câmbio, está implementado um Plano de Ação e de resposta a incidentes abrangendo o seguinte:

- As ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética.
- Os procedimentos, rotinas, controles e tecnologias a serem utilizadas na prevenção e na resposta a incidentes.
- Área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O Plano de Ação e de Resposta a Incidentes será aprovado pelo Diretor responsável pela Política Cibernética e será revisado no mínimo anualmente.

5.2. RELATÓRIO SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Será emitido anualmente, com data base de 31 de dezembro, relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes.

Esse Relatório deve contemplar, no mínimo, as seguintes informações:

- a efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética;

- o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- os resultados obtidos com os testes realizados nas ações previstas nesta Política e do Plano de Ação e de Resposta a Incidentes para a prevenção de incidentes cibernéticos.

O relatório deve ser elaborado até 31 de março do ano seguinte ao da data base devendo ser aprovado pelo Diretor responsável pela Segurança Cibernética.

6. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Os Prestadores de serviços e parceiros de serviços de processamento de dados e armazenamento em nuvem podem representar uma fonte significativa de riscos de cibersegurança.

A computação em nuvem considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações, envolve determinados riscos que são levados em conta pela Corretora, demandando assim cuidados proporcionais a esta identificação de ameaças.

6.1 EXIGÊNCIAS PARA A CONTRATAÇÃO DE SERVIÇOS

A Executive Corretora de Câmbio ao realizar contratações de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende às seguintes exigências:

- a) Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo:
 - Se mantém Política de Segurança da Informação
 - Se possui Plano de Continuidade Operacional
 - Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças)
 - Se mantém Gestão de Incidentes

b) Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:

- Cumprimento da legislação e da regulamentação em vigor
- Permissão de acesso da Executive Corretora de Câmbio aos dados e as informações a serem processadas ou armazenadas pelo Prestador de serviços.
- Confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviços.
- Aderência a certificações que a Executive Corretora de Câmbio possa exigir para a prestação do serviço a ser contratado.
- Acesso da Executive Corretora de Câmbio aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados.
- Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados.
- Identificação e segregação dos dados dos clientes da Executive Corretora de Câmbio por meio de controles físicos ou lógicos.

Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da Executive Corretora de Câmbio.

6.2 AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS

Executive Corretora de Câmbio deve proceder a uma avaliação da relevância dos serviços prestados por empresas com possibilidades de serem contratadas considerando o seguinte:

- criticidade dos serviços a serem prestados
- sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada.
- verificação quanto a adoção, por parte do prestador de serviços quanto a adoção de controles que mitiguem efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados através de internet.

6.3. COMUNICAÇÕES AO BANCO CENTRAL

A Executive Corretora de Câmbio deverá informar ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deve ser realizada *até dez dias após a contratação dos serviços* e deve conter as seguintes informações:

- a) denominação da empresa a ser contratada;
- b) os serviços relevantes a serem contratados;
- c) a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, nos casos de contratação no exterior.

As alterações contratuais que impliquem modificações nas informações contratuais devem ser comunicadas ao Banco Central *até dez dias após a alteração contratual*.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, deve observar os seguintes requisitos:

- a) a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- b) assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;
- c) definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e
- d) prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anterior a Executive Corretora de Câmbio deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas.

A Executive Corretora de Câmbio deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem

impedem o acesso das instituições contratantes e do Banco Central do Brasil aos dados e às informações.

6.4. DOS CONTRATOS

Os contratos firmados entre a Executive Corretora de Câmbio e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

- a) a indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- b) a adoção de medidas de segurança para a transmissão e armazenamento dos dados.
- c) a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes.
- d) a obrigatoriedade, em caso de extinção do contrato, de:
 - Transferência dos dados ao novo prestador de serviços ou a Executive Corretora de Câmbio.
 - Exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade
- e) O acesso da Executive Corretora de Câmbio a:
 - informações fornecidas pela empresa contratada visando verificar o cumprimento dos itens previstos nos itens a), b) e c) acima.
 - informações relativas às Certificações exigidas pela Corretora e aos relatórios de auditoria especializada contratada pelo prestador de serviços.
 - informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.
- f) a obrigação da empresa contratada notificar a Executive Corretora de Câmbio sobre a subcontratação de serviços relevantes para a Corretora.
- g) a permissão de acesso do Banco Central do Brasil às seguintes informações:
 - contratos e acordos firmados para a prestação de serviços
 - documentação e informações referentes aos serviços prestados
 - os dados armazenados
 - as informações sobre processamento

- as cópias de segurança dos dados e das informações
 - códigos de acesso aos dados e as informações.
- h) a adoção de medidas pela Executive Corretora de Câmbio em decorrência de determinação do Banco Central do Brasil
- i) a obrigatoriedade da empresa contratada em manter a Executive Corretora de Câmbio permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor.
- j) o contrato deve também prever, para o caso de decretação de regime de resolução da Corretora pelo Banco Central:
- A obrigação da empresa contratada para a prestação de serviços conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, a documentação e as informações referentes aos serviços prestados, aos dados armazenados e as informações sobre seus processos, as cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada.
 - A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observando que:
 - A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução.
 - A notificação prévia deve ocorrer também na situação em que a interrupção for motivada por inadimplência da Corretora.

7. PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO

7.1. MITIGAÇÃO DOS RISCOS E PROCEDIMENTOS DE CONTROLE

Está sendo estabelecido um conjunto de medidas buscando mitigar os riscos de forma a impedir previamente a ocorrência de um ataque cibernético e/ou vazamento de dados:

- A Corretora oferece aos Colaboradores uma completa estrutura tecnológica para o exercício das atividades, sendo responsabilidade de cada Colaborador manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (Computador, notebook, acesso à internet, E-mail etc.).
- Equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Corretora.
- A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da Corretora depende de autorização do Diretor responsável pela Política de Segurança Cibernética devendo observar os direitos de propriedade intelectual pertinentes, tais como copyright, licenças e patentes.
- As mensagens enviadas ou recebidas através do correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (internet) através de equipamentos da Corretora poderão ser monitoradas.
- As senhas para acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.) compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.
- As senhas são geradas com alta complexidade de combinação de caracteres através de sistema de geração de senhas pelo responsável pelo TI. Os usuários não podem alterar a própria senha e devem solicitar a alteração da mesma ao responsável caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

7.1.1. AUTENTICAÇÃO E GESTÃO DE IDENTIDADE

A Executive Corretora de Câmbio adota mecanismos de autenticação e gestão de identidade compatíveis com o nível de criticidade dos sistemas, a sensibilidade das informações tratadas e os riscos cibernéticos associados, observando as melhores práticas de segurança da informação e regulamentação vigente.

Assim, a autenticação de usuários e sistemas deverá observar os seguintes requisitos:

a) Uso obrigatório de autenticação multifator (MFA), combinando pelo menos dois fatores independentes de autenticação (conhecimento, posse ou característica biométrica), nos seguintes casos:

- acessos administrativos ou privilegiados;
- acessos remotos à infraestrutura tecnológica;
- acesso a sistemas críticos, sensíveis ou que tratem dados confidenciais.

b) Adoção de políticas de credenciais seguras, contemplando:

- requisitos mínimos de complexidade de senhas;
- periodicidade de expiração compatível com o risco;
- bloqueio automático após tentativas inválidas consecutivas;
- vedação ao compartilhamento de credenciais.

c) Utilização de mecanismos de autenticação diferenciados para sistemas críticos, podendo incluir certificados digitais, biometria ou tokens criptográficos.

A instituição manterá matriz formal de segregação de funções (SoD), com revisão periódica para mitigação de conflitos de interesse.

7.1.2. GESTÃO DE IDENTIDADE E ACESSO (IAM)

A Executive Corretora de Câmbio manterá processo estruturado de gestão de identidades e acessos, contemplando:

- a) Concessão de acessos baseada no princípio do menor privilégio e na necessidade de conhecimento (*need-to-know*);
- b) Segregação de funções críticas, de forma a prevenir conflitos de interesse e reduzir riscos operacionais e de fraude;
- c) Formalização do ciclo de vida de identidades e acessos, incluindo:
 - criação;
 - alteração;
 - revisão periódica;
 - revogação tempestiva, especialmente em casos de desligamento ou mudança de função;
- d) Realização de revisões periódicas de acessos, no mínimo anuais, ou em periodicidade inferior conforme criticidade dos ativos;
- e) Controle e monitoramento de contas privilegiadas, com aplicação de mecanismos adicionais de segurança e auditoria; e
- f) Registro formal das aprovações de concessão e alteração de acessos, garantindo rastreabilidade e responsabilização.

7.1.3. REGISTRO, MONITORAMENTO E RASTREABILIDADE

A Executive Corretora de Câmbio assegurará a implementação de controles de registro e monitoramento de acessos, contemplando:

- a) Registro (log) detalhado de autenticações, tentativas de acesso, operações relevantes e atividades privilegiadas;
- b) Garantia de integridade, confidencialidade e disponibilidade dos logs, prevenindo alterações ou exclusões não autorizadas;
- c) Retenção dos registros em conformidade com a regulamentação aplicável e com prazos mínimos definidos pela instituição;
- d) Monitoramento contínuo de eventos de acesso, com identificação de comportamentos anômalos ou suspeitos;
- e) Disponibilização de trilhas de auditoria para fins de investigação, conformidade regulatória e suporte à resposta a incidentes.

7.1.4. CONTROLES COMPLEMENTARES

A Executive Corretora de Câmbio poderá adotar controles adicionais sempre que necessário, incluindo:

- soluções de gestão centralizada de identidade (IAM);
- autenticação federada e gestão de identidade digital;
- uso de *Single Sign-On (SSO)* com requisitos de segurança reforçados;
- revisão diferenciada para acessos de terceiros e prestadores de serviço.

7.1.5. SEGURANÇA NA INTEGRAÇÃO DE SISTEMAS (APIs)

A instituição assegura que todas as integrações de sistemas, incluindo aquelas realizadas com o Banco Central do Brasil (BACEN), SISCOM, Sistema de Pagamentos Brasileiro (SPB), parceiros e prestadores de serviço, sejam implementadas e mantidas de forma segura, resiliente e em conformidade com os requisitos regulatórios aplicáveis.

As integrações observarão, no mínimo, os seguintes requisitos:

a) Utilização obrigatória de canais de comunicação seguros e criptografados, por meio de protocolos atualizados (ex: TLS 1.2 ou superior), sendo vedado o uso de versões obsoletas ou vulneráveis;

b) Implementação de mecanismos de autenticação forte entre sistemas, incluindo:

- uso de certificados digitais;
- chaves criptográficas;
- tokens de autenticação;
- outros mecanismos equivalentes, conforme criticidade;

c) Restrição de acesso às APIs com base no princípio do menor privilégio, garantindo que apenas sistemas e usuários autorizados possam realizar integrações;

d) Implementação de mecanismos de controle de integridade e autenticidade dos dados trafegados, prevenindo alterações não autorizadas.

7.1.5.1. REGISTRO, MONITORAMENTO E RASTREABILIDADE

A Executive Corretora de Câmbio deverá garantir:

- a) Registro completo (logs) de todas as transações realizadas por meio de APIs, incluindo identificação de origem, destino, data, horário e conteúdo relevante;
- b) Monitoramento contínuo das integrações, com capacidade de detecção de atividades anômalas ou suspeitas;
- c) Garantia da integridade, confidencialidade e retenção dos registros para fins de auditoria e conformidade regulatória;
- d) Capacidade de rastreamento de operações realizadas por sistemas integrados.

As integrações deverão ser submetidas a:

- a) Testes periódicos de segurança, incluindo testes de vulnerabilidades e, quando aplicável, testes de intrusão;
- b) Avaliações de segurança sempre que houver alterações relevantes nos sistemas, interfaces ou processos integrados;
- c) Validação contínua da efetividade dos controles de segurança implementados.

Quanto a Gestão de Acessos e Governança a Executive Corretora de Câmbio deverá assegurar que:

- a) Todos os acessos via API sejam previamente autorizados, formalizados e registrados;
- b) Os acessos sejam revisados periodicamente, conforme criticidade da integração;
- c) Os terceiros envolvidos nas integrações atendam aos mesmos requisitos de segurança estabelecidos pela instituição;
- d) Exista gestão formal de credenciais utilizadas nas integrações, incluindo ciclo de vida, rotação e revogação.

Nesse contexto, são considerados como controles complementares:

- a) Implementação de mecanismos de limitação de requisições e proteção contra abusos;
- b) Utilização de ambientes segregados para desenvolvimento, testes e produção;
- c) Monitoramento de disponibilidade e resiliência das integrações;
- d) Integração dos controles de APIs com os processos de gestão de riscos, continuidade de negócios e resposta a incidentes.

Todos os acessos via APIs deverão ser devidamente autorizados, monitorados, controlados e auditáveis, garantindo aderência às exigências regulatórias e mitigação dos riscos cibernéticos associados.

7.1.6. CULTURA DE SEGURANÇA

A Executive Corretora de Câmbio promoverá, de forma contínua e estruturada, a disseminação da cultura de segurança cibernética entre colaboradores, prestadores de serviços e demais partes relevantes, com o objetivo de reduzir riscos e fortalecer o ambiente de controle interno.

A instituição manterá programa estruturado de capacitação, com:

- a) Trilhas de treinamento por perfil de acesso;
- b) Indicadores de participação e eficácia;
- c) Registro formal das capacitações;
- d) Monitoramento contínuo de desempenho.

A instituição deverá implementar programa contínuo de conscientização em segurança da informação, contemplando:

- a) Realização de treinamentos periódicos obrigatórios para todos os colaboradores, com conteúdo compatível com suas funções e níveis de acesso;
- b) Treinamentos específicos para perfis críticos, como usuários com acesso privilegiado ou atuação em sistemas sensíveis;
- c) Divulgação regular de orientações, políticas e boas práticas de segurança e simulação de testes, tais como:
 - Realização periódica de simulações de ataques cibernéticos, incluindo campanhas de *phishing*, engenharia social e outras ameaças comuns;
 - Avaliação dos resultados das simulações para identificação de vulnerabilidades comportamentais;
 - Implementação de ações corretivas com base nos resultados obtidos.

- d) Desenvolvimento de campanhas internas de segurança da informação, com foco na prevenção de incidentes e proteção de dados;
- e) Disseminação de alertas sobre ameaças emergentes e boas práticas;
- f) Incentivo ao comportamento seguro no uso de recursos tecnológicos;
- g) como medidas de avaliação e melhorias contínuas:
 - Monitoramento da efetividade das ações de conscientização;
 - Atualização periódica dos conteúdos e métodos de treinamento;
 - Integração da cultura de segurança com os processos de gestão de risco e segurança cibernética.
 - A cultura de segurança deverá ser tratada como componente essencial da gestão de riscos da instituição.

7.2. PROTEÇÃO DE DADOS

A INSTITUIÇÃO assegura conformidade com a Lei nº 13.709/2018 (LGPD), incluindo:

- a) Tratamento baseado em hipóteses legais;
- b) Garantia dos direitos dos titulares;
- c) Nomeação de Encarregado (DPO);
- d) Comunicação de incidentes de dados pessoais;
- e) Adoção de *privacy by design e by default*.

Os dados gerados pela INSTITUIÇÃO acerca de clientes, operações, posições, contábeis etc. são protegidos por FIREWALL do próprio sistema operacional, salienta-se que não são realizados acessos externos por clientes e funcionários. O único acesso externo, ocorre quando há necessidade de manutenção no sistema operacional da INSTITUIÇÃO sendo que para que ocorra esse acesso, se faz necessária a liberação, que é feita unicamente pelo responsável do TI após aprovação pelo Diretor de Segurança Cibernética.

Para evitar vazamento de dados internos e informações não é permitido que os colaboradores disponham de quaisquer dados internos e restritos para fins diversos da sua atividade profissional.

Não são permitidas a gravação de dados em dispositivos pessoais ou acesso a e-mails pessoais que possam facilitar o envio de informações para fora do ambiente da Instituição.

Os e-mails disponibilizados pela INSTITUIÇÃO são de uso estritamente profissional e podem ser monitorados para o fim de prevenir vazamento de dados.

Regras para utilização do Correio Eletrônico (e-mail):

A INSTITUIÇÃO fornecerá, a seu critério, contas de correio eletrônico (@INSTITUIÇÃO.com.br) aos seus funcionários. As Mensagens de correio eletrônico (e-mails) internos e externos devem ser de caráter profissional, devendo ser evitado o uso para fins particulares. Isso vale também para arquivos anexos.

Todas as mensagens recebidas de origem desconhecida com links e/ou anexos deverão ser eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos.

É proibido configurar e/ou manter configuradas contas de correio eletrônico de servidores externos, isto é, diferentes de (@INSTITUIÇÃO.com.br), nos programas gerenciadores de correio eletrônico instalados em computadores da INSTITUIÇÃO.

O conteúdo das mensagens enviadas através de contas de correio da INSTITUIÇÃO (@INSTITUIÇÃO.com.br) é de inteira responsabilidade do usuário que utiliza a conta e que possui a senha com acesso exclusivo à caixa postal e para envio de mensagens.

É proibida a utilização do e-mail para fins ilegais, transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis.

É proibida a utilização de e-mail para transmitir mensagens conhecidas como Spam, JunkMail, correntes ou a distribuição de mensagens em massa não solicitadas.

É terminantemente proibido ao Gestor do TI, administradores de rede e/ou correio eletrônico, ler mensagens de correio eletrônico de qualquer usuário quando estiver realizando serviços de manutenção e suporte, exceto quando em cumprimento de determinações da Diretoria da INSTITUIÇÃO para efeitos de auditoria.

Reserva-se a INSTITUIÇÃO o direito de auditar a utilização de suas contas de correio eletrônico da INSTITUIÇÃO (@INSTITUIÇÃO.com.br) fornecidas aos usuários, sem se caracterizar invasão de privacidade.

Regras para utilização da Internet na Rede Corporativa da INSTITUIÇÃO:

O acesso à Internet foi disponibilizado na INSTITUIÇÃO para viabilizar a busca de informações ou agilizar determinados processos de nossa empresa.

Todo o acesso à Internet através da rede corporativa da INSTITUIÇÃO poderá ser controlado com a realização de auditorias nas páginas consultadas. Poderão ser gerados relatórios com nomes, páginas consultadas, tempo de consulta.

Os usuários são responsáveis por toda a utilização da Internet em computadores iniciados com seu login e senha. Quando o usuário se afastar do computador deverá encerrar a sessão através do “logoff”, bloquear, reiniciar ou desligar o sistema.

É proibido aos usuários configurar ou alterar as configurações de rede e de acesso à Internet dos computadores da INSTITUIÇÃO, incluindo as seguintes configurações de rede: IP, DNS, WINS, Gateway, Proxy e a instalação ou reconfiguração de clientes Proxy.

Deve ser evitado o acesso a redes sociais e de relacionamento, enviar, baixar ou manter arquivos de imagens, músicas, vídeo, arquivos executáveis em geral, ou quaisquer outros de caráter pessoal.

Não é permitido o acesso a sites de Internet com conteúdo pornográfico, jogos, hacker ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança.

É proibido o acesso a sites, a instalação e a utilização de programas de troca de mensagens instantâneas ou arquivos do tipo: ICQ, MSN Messenger, Yahoo, Messenger, Bittorrent, Imesh, AudioGalaxy, AIM, Morpheus, Kaaza, Emule, Napster e outros, salvo quando autorizado pela diretoria.

A utilização de sites do tipo Proxy é proibida e será considerada falta grave. Sempre que os usuários, utilizando a Internet, tiverem acesso a materiais criminosos como pornografia infantil (arte, textos, figuras, cenas, imagens) e outros, mesmo que de maneira esporádica e involuntária, deverão entrar em contato imediatamente com o TI e/ou com o DGR - Departamento de Gestão de Risco da INSTITUIÇÃO.

Regras para utilização de Internet utilizando a rede WI-FI:

Usuários autorizados pelo TI poderão conectar computadores ou outros equipamentos portáteis e pessoais à Internet, utilizando as redes sem fio disponíveis, essas redes não têm acesso a rede da INSTITUIÇÃO, tendo somente acesso à internet, protegidas por senha.

Todo o acesso à Internet através da rede WiFi da INSTITUIÇÃO poderá ser controlado com a realização de auditorias nas páginas consultadas.

Os usuários são responsáveis por toda a utilização da Internet através da rede WiFi da INSTITUIÇÃO e poderão ser identificados e responsabilizados em caso de acesso indevido.

Penalidades:

O TI – Tecnologia da Informação da INSTITUIÇÃO alerta a todos os usuários que a instalação ou utilização de softwares não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando aos infratores à pena de detenção e multa.

Todos os usuários são responsáveis pelo uso correto das ferramentas eletrônicas de propriedade da INSTITUIÇÃO.

Todas as práticas que representam ameaças à segurança da informação serão tratadas com a aplicação de ações disciplinares.

Portanto, na ocorrência de infrações a este Manual, ou às determinações constantes de comunicações externas ou internas, ou mesmo às ordens de superiores hierárquicos, quando for o caso, ficam os infratores sujeitos às seguintes penalidades: advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e/ou outras medidas judiciais cabíveis.

Todos os usuários de informática por ocasião de sua admissão na INSTITUIÇÃO recebem uma cópia deste Manual, dando ciência de seu conteúdo.

A INSTITUIÇÃO se reserva o direito de atualizar, alterar, anular todas ou em parte, as normas aqui contidas a qualquer momento. Uma versão atualizada deste manual estará sempre disponível na pasta do Sistema de Manuais Internos, disponível na rede da INSTITUIÇÃO.

Sempre que houver alguma alteração ou atualização deste manual, os usuários serão comunicados para que tomem conhecimento do seu conteúdo.

Política de Backup:

Compete ao TI a responsabilidade pelas cópias de segurança (backups) dos dados de softwares críticos, e todos demais dados armazenados nos servidores de redes internas e na nuvem;

Os servidores na nuvem estão programados para sofrer backups diários, com retenção de 30 dias, e backups mensais com retenção de 6 meses. A execução dos backups é de responsabilidade da

empresa contratada para armazenamento em nuvem, cabe à equipe de TI da Executive, monitorar a efetivação desses backups;

As evidências dessas verificações deverão ser salvas e disponibilizadas para o compliance e auditoria interna quando requisitadas;

Os usuários devem manter, obrigatoriamente, os dados críticos da empresa nos servidores de redes;

É de responsabilidade exclusiva do usuário a cópia e a guarda dos dados gravados na estação local (“C”) de trabalho;

Deverão ocorrer testes de efetividade dos backups durante o monitoramento anual da tecnologia da informação e LGPD.

Política de antivírus:

A INSTITUIÇÃO utiliza o firewall nativo no sistema operacional Microsoft que bloqueia todas as portas no sentido “Internet >> INSTITUIÇÃO”, com exceção das portas redirecionadas para os servidores que precisam ser acessados durante a manutenção do sistema.

A INSTITUIÇÃO utiliza a solução de antivírus da Bitdefender. Para computadores com maiores níveis de acesso também é utilizado o WatchGuard Agent Endpoint que é uma camada extra de segurança, ambos gerenciados pela Teevo.

A solução é totalmente gerenciada pela Web e atualização diária.

Política de acesso ao servidor:

O acesso aos servidores é restrito ao TI – Tecnologia da Informação ou pessoas autorizadas, ficando permanentemente bloqueado.

Política de concessão de acesso à rede e aos sistemas:

O responsável pela área em que o profissional for alocado fará a avaliação dos acessos necessários e solicitará a inclusão de acesso ao Gestor de Compliance, registrando a solicitação em chamado ao TI com cópia para o Gestor de Compliance. O gestor da área verificará também e encaminhará chamado ao TI da necessidade de cancelamento de acessos de sua equipe. A área de TI será responsável pelo atendimento do chamado após liberação pelo Gestor de Compliance.

Procedimentos de acesso remoto ao servidor que abriga os sistemas da INSTITUIÇÃO:

Os acessos remotos apenas serão concedidos se necessário qualquer reparo nas bases de dados dos sistemas utilizados pela INSTITUIÇÃO.

A concessão de acesso deve atender aos seguintes procedimentos:

Fornecedor solicita acesso;

Um chamado é aberto ao TI para acompanhar a manutenção e o acesso é concedido através da aprovação do mesmo, pela TI.

O acesso é acompanhado via tela por um dos técnicos da área de TI.

O acesso é revogado após a manutenção e encerrado pela TI.

Todos os contratos com fornecedores possuem cláusula de sigilo de informações a que possam ter acesso.

Política de avaliação e compra de hardware e software:

Nenhum hardware ou software poderá ser adquirido e/ou instalado na INSTITUIÇÃO sem autorização de um de seus diretores, mediante assinatura ou visto autorizando o pagamento.

Antes de ser comprado, todo hardware e software será avaliado pelo gestor de TI da INSTITUIÇÃO e aprovado junto a diretoria, quanto a:

Viabilidade técnica e aderência à plataforma tecnológica;

Facilidade de manutenção;

Documentação;

Atendimento às necessidades da INSTITUIÇÃO.

Ao autorizar a compra/pagamento, o diretor de TI ou da Segurança Cibernética, efetuou as avaliações e verificou a procedência do hardware ou do software em questão.

Sempre que possível, os chamados softwares de prateleira (sistemas operacionais, editores de texto, planilhas e outros) serão adquiridos junto dos equipamentos ou sob forma de licença de uso, dando cobertura a cada cópia requerida conforme a necessidade.

Controles Criptográficos

A INSTITUIÇÃO adotará mecanismos criptográficos adequados para assegurar a confidencialidade, a integridade e a autenticidade das informações, compatíveis com o nível de criticidade dos ativos, a sensibilidade dos dados tratados e os riscos cibernéticos associados, em consonância com as melhores práticas de mercado e regulamentação vigente.

Proteção De Dados Em Trânsito

Os dados trafegados em redes internas e externas deverão ser protegidos por meio de protocolos criptográficos seguros, observando:

- a) Utilização obrigatória de protocolos seguros e atualizados (ex: TLS versão 1.2 ou superior), vedado o uso de versões obsoletas ou vulneráveis;
- b) Proteção de comunicações envolvendo:
 - acesso remoto;
 - integração entre sistemas internos e externos (incluindo BACEN, SISCOM, SPB e parceiros);
 - transmissão de dados sensíveis ou confidenciais;
- c) Implementação de mecanismos que garantam a autenticidade das partes envolvidas e a integridade dos dados transmitidos.

Proteção de Dados em Repouso

Os dados armazenados em servidores, estações de trabalho, dispositivos móveis ou ambientes em nuvem deverão ser protegidos por criptografia adequada, observando:

- a) Aplicação de algoritmos criptográficos reconhecidos e considerados seguros pelos padrões de mercado;
- b) Proteção obrigatória para:
 - bases de dados contendo informações sensíveis ou confidenciais;
 - backups e cópias de segurança;
 - mídias removíveis e dispositivos portáteis, quando aplicável;

c) Segregação lógica e controle de acesso aos dados criptografados, de forma a impedir acesso não autorizado.

Gestão De Chaves Criptográficas

A INSTITUIÇÃO manterá controles formais para gestão do ciclo de vida das chaves criptográficas, incluindo:

- a) Geração, distribuição, armazenamento, rotação e revogação de chaves de forma segura;
- b) Restrição de acesso às chaves criptográficas apenas a usuários e sistemas devidamente autorizados, com base no princípio do menor privilégio;
- c) Proteção das chaves contra acesso indevido, perda, divulgação ou uso não autorizado;
- d) Registro e rastreabilidade de todas as operações relevantes envolvendo chaves criptográficas;
- e) Adoção de práticas seguras para armazenamento, podendo incluir uso de cofres digitais, HSM (Hardware Security Module) ou mecanismos equivalentes, quando aplicável.

Controles Complementares

Como complemento aos controles criptográficos, a INSTITUIÇÃO deverá:

- a) Monitorar continuamente o uso de mecanismos criptográficos e eventuais vulnerabilidades conhecidas;
- b) Atualizar periodicamente os algoritmos, protocolos e práticas criptográficas, de modo a evitar obsolescência tecnológica;
- c) Garantir que prestadores de serviços e terceiros que tratem dados da instituição adotem controles criptográficos compatíveis com os padrões estabelecidos;
- d) Assegurar que a utilização de criptografia esteja formalmente documentada e alinhada à classificação das informações da INSTITUIÇÃO.

Os controles aqui estabelecidos deverão ser periodicamente avaliados quanto à sua efetividade, sendo atualizados sempre que necessário para atendimento à evolução das ameaças cibernéticas e exigências regulatórias.

7.3. AÇÕES DE PREVENÇÃO

Devem ser criados mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade da segurança cibernética da Corretora através das seguintes ações:

- Manter inventários atualizados de hardware e software, bem como verificá-los com frequência para identificar elementos estranhos à instituição. Por exemplo, computadores não autorizados ou software não licenciado.
- Manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.
- Monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.
- Realizar, periodicamente testes de invasão externa e *phishing*
- Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.
- Anualmente testar as ações do plano de resposta a incidentes, simulando os cenários quando possível e registrar os testes obtidos em relatório.

Nesse contexto, a instituição deverá assegurar:

- Testes periódicos independentes;
- Auditorias internas e externas;
- Plano anual de testes;
- Reporte formal à alta administração;
- Acompanhamento de planos de ação.

7.3.1. GESTÃO DE VULNERABILIDADES

A instituição deverá manter processo estruturado, contínuo e formal de gestão de vulnerabilidades, com o objetivo de identificar, avaliar, tratar e monitorar fragilidades nos ativos

tecnológicos que possam comprometer a confidencialidade, integridade e disponibilidade das informações, em conformidade com as melhores práticas de mercado e regulamentação vigente.

7.3.2. IDENTIFICAÇÃO DE VULNERABILIDADES

A identificação de vulnerabilidades deverá contemplar:

a) Execução periódica de varreduras automatizadas de vulnerabilidade (scans) em:

- redes internas e externas;
- servidores, estações de trabalho e dispositivos móveis;
- sistemas e aplicações críticas;
- ambientes em nuvem e integrações com terceiros;

b) Realização de testes de intrusão (pentests) de forma periódica ou sempre que houver mudanças relevantes no ambiente tecnológico;

c) Monitoramento contínuo de fontes confiáveis de ameaças e vulnerabilidades conhecidas (ex: boletins de segurança de fabricantes, bases públicas e privadas);

d) Identificação de vulnerabilidades decorrentes de falhas de configuração, softwares desatualizados ou uso inadequado de recursos tecnológicos.

7.3.3. AVALIAÇÃO E CLASSIFICAÇÃO DE RISCOS

As vulnerabilidades identificadas deverão ser avaliadas e classificadas conforme metodologia definida pela instituição, considerando:

- a) Nível de criticidade do ativo afetado;
- b) Facilidade de exploração da vulnerabilidade;
- c) Potencial impacto operacional, financeiro, regulatório e reputacional;
- d) Existência de controles compensatórios.

7.3.3.1. METODOLOGIA DE CLASSIFICAÇÃO DE RISCOS CIBERNÉTICOS

A Executive Corretora de Câmbio estabelece metodologia formal de gestão e classificação de riscos cibernéticos, alinhada à sua estrutura de gerenciamento de riscos corporativos.

Os riscos cibernéticos serão avaliados com base, no mínimo, nos seguintes critérios:

- a) Probabilidade de ocorrência;
- b) Impacto potencial, incluindo:
 - impacto operacional;
 - impacto financeiro;
 - impacto regulatório;
 - impacto reputacional;
- c) Nível de exposição a ameaças externas e internas;
- d) Efetividade dos controles existentes.

Os riscos deverão ser classificados em níveis (ex: Baixo, Médio, Alto, Crítico), sendo formalmente registrados e monitorados.

A instituição deverá definir e aprovar apetite e tolerância ao risco cibernético, assegurando alinhamento com seus objetivos estratégicos.

A classificação deverá, no mínimo, contemplar níveis de severidade (ex: crítico, alto, médio, baixo).

7.3.4. TRATAMENTO E REMEDIAÇÃO

A instituição deverá estabelecer procedimentos formais para tratamento das vulnerabilidades, incluindo:

- a) Definição de prazos máximos para correção, compatíveis com o nível de criticidade identificado;
- b) Adoção de medidas corretivas como:
 - aplicação de patches e atualizações de segurança;
 - ajustes de configuração (hardening);
 - substituição de componentes vulneráveis;
 - implementação de controles compensatórios, quando a correção imediata não for possível;
- c) Priorização da remediação de vulnerabilidades críticas, com tratamento tempestivo e acompanhamento contínuo;
- d) Validação da correção realizada por meio de novas verificações ou testes específicos.

7.3.5. REGISTRO, MONITORAMENTO E GOVERNANÇA

A INSTITUIÇÃO deverá garantir o registro, controle e monitoramento contínuo das vulnerabilidades, contemplando:

- a) Registro formal de todas as vulnerabilidades identificadas, suas classificações e status de tratamento;
- b) Acompanhamento sistemático das ações de correção até sua completa resolução;
- c) Manutenção de evidências das ações realizadas para fins de auditoria e conformidade;
- d) Reporte periódico à alta administração ou instância responsável sobre o status das vulnerabilidades e riscos associados;
- e) Integração do processo de gestão de vulnerabilidades com a gestão de riscos, resposta a incidentes e continuidade de negócios.

Como parte da gestão de vulnerabilidades, a Executive Corretora de Câmbio deverá ainda:

- a) Garantir a atualização regular de sistemas operacionais, aplicações e componentes tecnológicos;
- b) Avaliar vulnerabilidades relacionadas a prestadores de serviços e terceiros que tratem dados ou operem sistemas da instituição;
- c) Revisar periodicamente a efetividade do processo de gestão de vulnerabilidades, promovendo melhorias contínuas;
- d) Assegurar que as práticas adotadas sejam proporcionais ao porte, complexidade e perfil de risco da instituição.

O processo de gestão de vulnerabilidades deverá ser executado de forma contínua e documentada, garantindo rastreabilidade, consistência e aderência às exigências regulatórias aplicáveis.

7.3.5.1. INTEGRAÇÃO COM GESTÃO DE RISCOS

A gestão de riscos cibernéticos integra o framework de gerenciamento de riscos da instituição, em conformidade com as normas do Banco Central do Brasil.

Essa integração contempla:

- a) Incorporação dos riscos cibernéticos ao mapa de riscos corporativo;

- b) Avaliação periódica pelo Comitê de Riscos ou instância equivalente;
- c) Integração com gestão de riscos operacionais;
- d) Comunicação tempestiva à alta administração sobre riscos relevantes;
- e) Alinhamento com controles internos e compliance.

Os riscos cibernéticos devem ser considerados no processo decisório da instituição.

7.3.6. REGISTROS E RASTREABILIDADE

A INSTITUIÇÃO manterá trilhas de auditoria (logs) que permitam:

- Identificação de acessos e ações realizadas nos sistemas;
- Detecção de atividades suspeitas;
- Retenção de registros por prazo mínimo de 5 anos, conforme regulamentação.
- Os logs devem ser protegidos contra alterações e acessados apenas por pessoal autorizado.

7.4. TRATAMENTO DE INCIDENTES

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da Corretora, como por exemplo:

- queda de energia elétrica
- falha de um elemento de conexão
- servidor fora do ar
- ausência de conexão com internet
- sabotagem / terrorismo
- Indisponibilidade de acesso a corretora
- Ataques DDOS

Qualquer funcionário que detectar um incidente deverá comunicar imediatamente as demais áreas sobre o fato, para que o mesmo seja levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

AValiação Inicial

Avaliar o incidente em conjunto com a Diretoria para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas.

Analisar motivos e consequências imediatas, bem como a gravidade da situação.

INCIDENTE CARACTERIZADO

Caracterizado o incidente, devem ser tomadas as medidas imediatas, tais como:

- Iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros.
- O Diretor responsável pela Política de Segurança Cibernética avaliará junto com a equipe de TI o impacto do incidente nos diversos riscos envolvidos.
- Conforme a relevância (sabotagem, terrorismo etc.) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providências.

Conforme a relevância do incidente comunicar os clientes que porventura tenham sido afetados.

RECUPERAÇÃO

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência de TI acionada e terceiros-chave notificados.

Quaisquer dados faltando ou corrompidos, ou problemas identificados por colaboradores internos devem ser comunicados à Diretoria e ao Diretor responsável pela Política de Segurança Cibernética.

RETOMADA

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

COMPARTILHAMENTO DE INCIDENTES

A INSTITUIÇÃO deverá estabelecer diretrizes formais para o compartilhamento de informações relativas a incidentes cibernéticos relevantes, observando os requisitos legais, regulatórios e de confidencialidade aplicáveis.

COMPARTILHAMENTO COM AUTORIDADES E REGULADORES

A INSTITUIÇÃO deverá realizar:

- a) Comunicação de incidentes relevantes ao Banco Central do Brasil, quando aplicável, conforme regulamentação vigente;
- b) Disponibilização de informações necessárias para investigação e supervisão regulatória;
- c) Atendimento tempestivo às solicitações das autoridades competentes, nos termos das regulamentações e leis aplicáveis a INSTITUIÇÃO.

COMPARTILHAMENTO COM OUTRAS INSTITUIÇÕES, ENTIDADES E PRESTADORES DE SERVIÇOS

No contexto de compartilhamento com outras instituições e entidades a INSTITUIÇÃO, deverá:

- a) Quando aplicável, compartilhamento de informações com outras instituições financeiras ou organismos especializados, visando a prevenção de riscos sistêmicos;
- b) Compartilhamento preferencialmente anonimizado, sempre que possível, para preservação de informações sensíveis;
- c) Comunicação a prestadores de serviços e terceiros envolvidos, quando necessário à contenção, mitigação ou solução do incidente;
- d) Garantia de alinhamento com as obrigações contratuais e requisitos de segurança estabelecidos.

REQUISITOS DE CONFIDENCIALIDADE E PROTEÇÃO

São considerados requisitos de confidencialidade e proteção:

- a) O compartilhamento deverá respeitar a legislação aplicável, incluindo normas de sigilo bancário e proteção de dados;

- b) As informações compartilhadas deverão ser limitadas ao estritamente necessário;
- c) Deverão ser adotadas medidas para proteger a integridade e confidencialidade das informações compartilhadas.

REGISTRO E GOVERNANÇA

Todos os compartilhamentos realizados deverão ser formalmente registrados, bem como mantida rastreabilidade das informações compartilhadas e das entidades envolvidas.

A instituição deverá revisar periodicamente os procedimentos de compartilhamento. O compartilhamento de incidentes deverá contribuir para o fortalecimento da resiliência cibernética da instituição e do sistema financeiro como um todo.

7.5 INTELIGÊNCIA EM CIBERSEGURANÇA

A instituição deverá estabelecer processo contínuo e estruturado de inteligência em cibersegurança, com o objetivo de identificar, analisar e responder proativamente a ameaças cibernéticas relevantes, mitigando riscos à confidencialidade, integridade e disponibilidade das informações e dos ativos tecnológicos.

Esse processo deverá ser compatível com o porte, a complexidade, o modelo de negócio e o perfil de risco da instituição, especialmente no contexto de suas operações no Sistema Financeiro Nacional.

A instituição deverá monitorar de forma contínua fontes de informação confiáveis sobre ameaças cibernéticas, incluindo:

a) fontes públicas, como:

- bases de vulnerabilidades e incidentes conhecidos;
- comunicados de segurança de fabricantes de software e hardware;
- publicações de órgãos reguladores e entidades especializadas;

b) fontes privadas, quando aplicável, como:

- serviços especializados em inteligência de ameaças;
- fornecedores de tecnologia e segurança da informação;

- redes de compartilhamento de informações entre instituições financeiras;

c) informações relacionadas a ameaças emergentes, campanhas de ataques, técnicas, táticas e procedimentos (TTPs) utilizados por agentes maliciosos.

As informações coletadas deverão ser analisadas de forma estruturada, contemplando:

a) Avaliação da relevância das ameaças identificadas em relação ao ambiente tecnológico da instituição;

b) Identificação de possíveis vulnerabilidades exploráveis no contexto interno;

c) Análise do impacto potencial sobre:

- operações de câmbio e integrações com sistemas (ex: BACEN, SISCOM, SPB);
- dados de clientes e informações sensíveis;
- continuidade dos serviços e reputação da instituição;

d) Classificação do risco associado às ameaças identificadas, com priorização para tratamento.

Com base na análise realizada, a instituição deverá adotar medidas preventivas e corretivas adequadas, incluindo:

a) Atualização de sistemas, aplicações e mecanismos de segurança;

b) Ajustes de configuração em ativos tecnológicos;

c) Implementação de regras de bloqueio e detecção em ferramentas de segurança;

d) Reforço de controles de acesso e autenticação;

e) Revisão de integrações com sistemas externos e terceiros, quando aplicável.

A instituição poderá compartilhar, quando aplicável e observadas as restrições legais e de confidencialidade:

a) Informações sobre ameaças e incidentes relevantes com o Banco Central do Brasil;

b) Dados agregados ou anonimizados com outras instituições financeiras ou fóruns especializados;

c) Informações com prestadores de serviços essenciais, quando necessário à mitigação de riscos.

O processo de inteligência em cibersegurança deverá estar integrado com:

- a) Gestão de vulnerabilidades;
- b) Monitoramento de eventos e incidentes;
- c) Gestão de riscos operacionais e cibernéticos;
- d) Plano de resposta a incidentes e continuidade de negócios.

A instituição deverá garantir controle de governança e monitoramento, no que tange a:

- a) Registro e documentação das atividades de inteligência realizadas;
- b) Monitoramento contínuo da efetividade das ações adotadas;
- c) Revisão periódica das fontes de informação e dos processos estabelecidos;
- d) Reporte à alta administração ou instância responsável, quando aplicável.

O processo de inteligência em cibersegurança deverá ser continuamente aprimorado, de forma a acompanhar a evolução das ameaças e garantir a resiliência da instituição frente ao cenário de riscos cibernéticos.

7.6. MONITORAMENTO E TESTES

O ambiente de TI da Corretora deve ser supervisionado e monitorado com o objetivo de verificar sua efetividade e detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

É possível a ocorrência de algum risco de segurança cibernética através de uma das seguintes situações descritas:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas;
- Comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”)
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com condições internamente estabelecidas.
- Vazamento de informações durante tráfego de dados não criptografados.

Anualmente a Corretora deve providenciar a execução de testes de cibersegurança através da verificação dos seguintes itens:

- Uso da capacidade instalada da rede e dos equipamentos, bem como capacidade e efetividade do armazenamento em nuvem;
- Tempo de resposta no acesso à internet e aos sistemas críticos da Corretora;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Corretora;
- Vulnerabilidades que possam causar incidentes (vírus, trojans, furtos, acessos indevidos etc.);
- Inspeção física nas máquinas de hardware, se mantido servidor físico.

8. CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

A instituição mantém Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (DRP), visando assegurar a continuidade das operações críticas.

Os planos contemplam:

- a) Identificação de processos críticos;
- b) Definição de RTO e RPO;
- c) Estratégias de contingência tecnológica;
- d) Procedimentos de recuperação de sistemas;
- e) Estruturas alternativas de operação;
- f) Testes periódicos de efetividade.

Os planos são revisados anualmente e integrados ao Plano de Resposta a Incidentes.

9. MONITORAMENTO, INDICADORES E REPORTE DE SEGURANÇA CIBERNÉTICA

A Executive Corretora de Câmbio deverá estabelecer e manter processo estruturado de monitoramento da efetividade da segurança cibernética, por meio da definição, acompanhamento e reporte de indicadores de desempenho (KPIs) e indicadores de risco (KRIs).

Os indicadores deverão permitir a avaliação contínua da eficácia dos controles, da exposição a riscos cibernéticos e da capacidade de resposta da instituição a incidentes.

Devem ser considerados, no mínimo:

a) Indicadores de Desempenho (KPIs):

- tempo médio de detecção e resposta a incidentes;
- percentual de vulnerabilidades corrigidas dentro do prazo;
- disponibilidade de sistemas críticos;
- taxa de sucesso em testes de continuidade e recuperação;

b) Indicadores de Risco (KRIs):

- volume e criticidade de vulnerabilidades abertas;
- número de incidentes relevantes;
- tentativas de acesso indevido ou ataques detectados;
- taxa de falhas em simulações de phishing;

c) Indicadores de Cultura e Conscientização:

- taxa de participação em treinamentos;
- nível de aderência às políticas de segurança.

Os indicadores deverão:

- Ser monitorados continuamente pela área responsável;
- Ser reportados periodicamente à alta administração;
- Subsidiar processos de tomada de decisão;
- Permitir a identificação de tendências e riscos emergentes.

Os resultados deverão ser formalmente documentados e utilizados para promover a melhoria contínua da segurança cibernética da instituição, em alinhamento com sua estratégia e com seu apetite de risco.

10. DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

- Política de Segurança Cibernética;
- Ata de Reunião da Diretoria da Corretora implementado a Política de Segurança Cibernética;
- Documento relativo ao Plano de Ação e de resposta a incidentes relativos à implementação da Política de Segurança Cibernética;
- Relatório anual sobre a implementação do Plano de ação e de resposta a incidente;
- Documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;

Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra;

- Contratos de Prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem;
- Dados, registros e informações relativas aos mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

11. REGULAMENTAÇÃO ASSOCIADA

Resolução CMN nº 4.893 de 26 de fevereiro de 2021.

Além das normas citadas, esta Política observa:

- Resolução CMN nº 4.557/2017 (Gestão de Riscos);
- Resoluções CMN nº 5.117/2024 e 5.274/2025;
- Circular BCB nº 3.978/2020 (PLD/FT);
- Lei nº 13.709/2018 (LGPD);
- Lei nº 12.965/2014 (Marco Civil da Internet).

12. ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA

O conteúdo desta Política de Segurança Cibernética aplica-se a todos os funcionários e prestadores de serviços relevantes da Executive Corretora de Câmbio, no âmbito de suas atividades, atribuições e responsabilidades.

Está aprovada pela Diretoria a qual está comprometida com a melhoria contínua do disposto neste normativo.

Está sendo publicada e comunicada para todos os funcionários, empresas contratadas de serviços de cibernética e clientes e partes externas relevantes, para o necessário cumprimento.

Um resumo da Política de Segurança Cibernética estará sendo divulgado ao público através do site da Corretora.

É obrigação de cada funcionário conhecer e praticar as disposições desta Política e assegurar que, quando necessário, prestadores de serviços sejam informados sobre as regras estabelecidas. Treinamentos e divulgações internas regulares sobre o tema serão realizadas para garantir a capacitação sobre as diretrizes desta Política.

Esta Política, juntamente com o Plano de Ação e respostas a incidentes será revisada anualmente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia.