Fourtrade

Corretora de Câmbio

Política de Segurança Cibernética e proteção de dados
Revisão 00

Área Responsável	Data	Revisão
Departamento de Informática	23/07/2024	00
Assunto:		
Política de Segurança Cibernética e proteção de dados		

ÍNDICE

Área Responsável	Data	Revisão
Departamento de Informática	23/07/2024	00
Assunto:		
Política de Segurança Cibernética e proteção de dados		

1. OBJETIVO

A Política de Segurança Cibernética e proteção de dados da **FOURTRADE CORRETORA DE CÂMBIO LTDA** tem como objetivo 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 cyber segurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo de nossos negócios, bem como estabelecer os princípios gerais, as diretrizes e as responsabilidades relacionados à 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 4.893/2021.

2. FUNÇÕES E RESPONSABILIDADES

DIRETOR RESPONSÁVEL PELA POLÍTICA DE SEGURANÇA CIBERNÉTICA E EXECUÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

- Revisar e aprovar a política de Segurança Cibernética;
- Estabelecer diretrizes, orientações e controles que permitem a administração e a outros funcionários conduzir suas responsabilidades nos termos da política.
- Prover os meios necessários para que as atividades relacionadas segurança cibernética sejam exercidas adequadamente.
- Receber, analisar e tomar providências em relação ao reporte de resultados decorrentes das atividades relacionadas à segurança cibernética, de possíveis irregularidades ou falhas identificadas.
- Garantir que medidas corretivas sejam tomadas na identificação de falhas.
- Executar o 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.

ADMINISTRADORES, FUNCIONÁRIOS, COLABORADORES E TERCEIROS

- Observar e zelar pelo cumprimento da presente Política e, quando assim se fizer necessário, acionar o encarregado de Proteção de Dados ou Data Protection Officer (DPO) para consulta sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas.

COMPLIANCE

- Manter atualizada esta Política, de forma a garantir que quaisquer alterações regulatórias/legais das diretrizes e regras gerais aqui estabelecidas sejam observadas;
- Esclarecer dúvidas relativas a esta Política e à sua aplicação;

- Aceitar reclamações, prestar esclarecimentos e adotar providências;
- Receber comunicações da Autoridade Nacional de Proteção de Dados ("ANPD") e dos órgãos reguladores adotando providências;
- Orientar os funcionários, colaboradores e os terceiros da Corretora a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Adotar iniciativas para compartilhamento de informações sobre incidentes contendo dados pessoais com a Autoridade Nacional de Proteção de Dados ("ANPD") e com os titulares dos dados, quando necessário.

ENCARREGADO PELO TRATAMENTO DE DADOS (DPO – DATA PROTECTION OFFICER)

- Informar e aconselhar o responsável pelo tratamento e os demais profissionais sobre suas obrigações da LGPD;
- Controlar a conformidade com o LGPD e com as políticas do responsável pelo tratamento, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal envolvido no tratamento;
- Prestar aconselhamento, se tal for solicitado, no que se refere à avaliação do impacto da proteção de dados, e acompanhar o seu desempenho;
- Cooperar com as autoridades;
- Servir de ponte para a autoridade de supervisão em questões relacionadas com o tratamento;
- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

AUDITORIA INTERNA

- Analisar se a Corretora está com os procedimentos adequados e alinhados com esta política e a lei LGPD.

3. DIRETRIZES

A Política de Segurança Cibernética e proteção de dados da Fourtrade Corretora de Câmbio baseia-se nos seguintes princípios:

a. 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.

b. 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);

c. 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:

a. O porte, perfil de risco e o modelo de nossos negócios;

b. A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais.

c. 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.

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

a. Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a Fourtrade Corretora de Câmbio implantar ou executar *softwares*, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos.

b. Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela Fourtrade Corretora de Câmbio utilizando recursos computacionais de seus prestadores de serviços.

c. Execução por meio de Internet dos aplicativos implantados ou desenvolvidos por prestadores de serviços da Fourtrade Corretora de Câmbio, com utilização de recursos computacionais do próprio prestador de serviços contratado pela Corretora.

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

a. Análises de informações e de recursos adequados ao monitoramento dos serviços;

b. Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a Prestadores de serviços; e

c. Cumprimento da legislação e da regulamentação vigente.

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

Empresas fornecedores 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.

4.1 AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS

A Fourtrade Corretora de Câmbio deve proceder com a 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; e
- 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.

4.2 EXIGÊNCIAS PARA A CONTRATAÇÃO DE SERVIÇOS

AO realizar contratações de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, a Fourtrade Corretora de Câmbio 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:

   i. Se mantém Política de Segurança da Informação;

   ii. Se possui Plano de Continuidade Operacional;

   iii. Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças); e

   iv. Se mantém Gestão de Incidentes.

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

   v. Cumprimento da legislação e da regulamentação em vigor;

   vi. Permissão de acesso da Fourtrade Corretora de Câmbio aos dados e as informações a serem processadas ou armazenadas pelo Prestador de serviços;

   vii. Confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas ou armazenadas pelo Prestador de serviços;

   viii. Aderência a certificações que a Fourtrade Corretora de Câmbio possa exigir para a prestação do serviço a ser contratado;

ix. Acesso da Fourtrade 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;

x. Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;

xi. Identificação e segregação dos dados dos clientes da Fourtrade Corretora de Câmbio por meio de controles físicos ou lógicos;

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

4.3 COMUNICAÇÃO AO BANCO CENTRAL

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

Essa comunicação deve ser realizada 60 dias antes da contratação dos serviços e deve conter as seguintes informações:

a. Denominação da empresa a ser contratada;

b. Os serviços relevantes a serem contratados; e

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 no mínimo 60 dias antes da alteração contratual.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada pela, 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 Fourtrade Corretora de Câmbio deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas.

A Fourtrade 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.

4.4 DOS CONTRATOS

Os contratos firmados entre a Fourtrade 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:

   i. Transferência dos dados ao novo prestador de serviços ou a Fourtrade Corretora de Câmbio;

   ii. Exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade;

e. O acesso da Fourtrade Corretora de Câmbio à:

   i. Informações fornecidas pela empresa contratada visando verificar o cumprimento dos itens previstos nos itens a), b) e c) acima;

   ii. Informações relativas às Certificações exigidas pela Corretora e aos relatórios de auditoria especializada contratada pelo prestador de serviços.

   iii. Informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.

f. A obrigação da empresa contratada notificar a Fourtrade 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:

   i. Contratos e acordos firmados para a prestação de serviços

   ii. Documentação e informações referentes aos serviços prestados

   iii. Os dados armazenados

   iv. As informações sobre processamento

   v. As cópias de segurança dos dados e das informações

   vi. Códigos de acesso aos dados e as informações.

h. A adoção de medidas pela Fourtrade Corretora de Câmbio em decorrência de determinação do Banco Central do Brasil;

i) A obrigatoriedade de a empresa contratada manter a Fourtrade Corretora de Câmbio permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor.

i. O contrato deve também prever, para o caso de decretação de regime de resolução da Corretora pelo Banco Central:

   i. 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.

   ii. 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:

      1. 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 motivava por inadimplência da Corretora.

5. PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO

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; e
- 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.

Com isso, os ativos incorporados no espaço cibernético devem ser protegidos e preservados, sendo também este, 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; e
- Componentes físicos, como servidores, estações de trabalho, notebooks, etc

5.1 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:

a. 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;

b. Manter os sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas;

c. Monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados;

d. Realizar, periodicamente testes de invasão externa e *Phishing*;

e. Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura; e

f. Periodicamente testar o plano de resposta a incidentes, simulando os cenários.

5.2 MITIGAÇÃO DOS RISCOS

Nesta política a Fourtrade Corretora de Câmbio estabelece um conjunto de medidas buscando mitigar os riscos de um ataque cibernético.

É oferecido aos colaboradores estrutura tecnológica completa para o exercício das atividades, sendo responsabilidade destes 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.

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) e seus respectivos anexos, assim como os aplicativos de mensagens dos celulares corporativos e a navegação através da rede mundial de computadores (internet) através de equipamentos da Corretora poderão ser monitorados.

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.

Área Responsável	Data	Revisão
Departamento de Informática	23/07/2024	00
Assunto:		
Política de Segurança Cibernética e proteção de dados		

6. 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; e
- 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.

O processo de tratamento de incidentes pode ocorrer da seguinte forma?

AVALIAÇÃO INICIAL

Fase de avaliação inicial do 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 e ou as Filiais, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros;
- Submeter o ocorrido ao diretor responsável pela Política de Segurança Cibernética para avaliação do impacto do incidente e dos diversos riscos envolvidos;
- Registrar boletim de ocorrência ou queixa crime para as devidas providências, conforme a relevância (sabotagem, terrorismo, etc.); e
- Comunicar os clientes que por ventura tenham sido afetados, conforme a relevância do incidente.

RECUPERAÇÃO

Fase iniciada 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 T.I e ao Diretor responsável pela Política de Segurança Cibernética.

RETOMADA

Fase referente 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.

7. 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:

a. Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de *hackers*;

b. Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas;

c. Comprometimento de estações de trabalho decorrente de cliques em *link* malicioso (“*Phishing*”);

d. Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com condições internamente estabelecidas;

e. Vazamento de informações durante tráfego de dados não criptografados;

f. Semestralmente a Corretora deve providenciar a execução de testes de cibersegurança através da verificação dos seguintes itens:

g. Uso da capacidade instalada da rede e dos equipamentos;

h. Tempo de resposta no acesso à internet e aos sistemas críticos da Corretora;

i. Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Corretora;

j. Vulnerabilidades que possam causar incidentes (vírus, trojans, furtos, acessos indevidos, etc.); e

k. Inspeção física nas máquinas de hardware, se mantido servidor físico.

8. 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; e
- 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.

9. ESTRUTURA OPERACIONAL – EQUIPAMENTOS E SISTEMAS

ENCARREGADO PELO TRATAMENTO DE DADOS (DPO – DATA PROTECTION OFFICER):

Oscar de Andrade Toquero

SISTEMA DE GERENCIAMENTO DE CÂMBIO

Intermediação/Posição Própria – VUORI – FX Câmbio – www.vuori.com.br

Responsáveis: Luciana Volante e Alexandre Reis de Sales

SISTEMA DE GERENCIAMENTO DE CÂMBIO

Turismo – VUORI – GN Câmbio – www.vuori.com.br

Responsável: Kelly Kyan

SISTEMA DE ASSINATURA ELETRONICA

Posição Própria – WEBCOMEX – VUORI – www.webcomex/Account/Login.aspx.

Responsável: Luciana Volante

SISTEMA DE PLD e FT

E-GUARDIAN – ADVICE - http://sql-server/login/

Responsável: Rogério Gonçalves

SISTEMA DE COMPLIANCE

RISC – ADVICE - https://www.advicetech.com.br/knonefrontnovo

Responsável: Rogério Gonçalves

SISTEMA DE CONSULTA TRIBUTÁRIA EM CÂMBIO

MARCA CONSULTORIA - www.marcaconsultoria.com.br

marca@marcaconsultoria.com.br

Responsável: Rui Cabral e Gisele Mello

SISTEMA DE INFORMAÇÕES DE MERCADO

ENFOQUE SISTEMA - www.enfoque.com.br

TELEFONIA

RJ – Intelig - Contingência – Nextel (4G)

SP – VIVO - Contingência – Claro, Nextel (4G)

MANUTENÇÃO DAS CENTRAIS TELEFÔNICAS

RJ – Golden Phone Sr. Carlos José/Paranhos carlosjose@goldennetworks.com.br

www.goldennetworks.com.br - Tel.: (21)2560-7660

SP - PactTelecom – Sr. Person Soriano person@pacttelecom.com.br

www.pacttelecom.com.br

Tel.: (11) 6823-9100 / (11) 9953-5809

NOTEBOOKS

A empresa possui 05 computadores portáteis com todos os programas instalados e pronto acesso para dar continuidade aos seus negócios.

As centrais do RJ e SP foram interligadas através de IP´s/VPN para realização de ligações interurbanas entre as praças.

A matriz no RJ tem disponíveis notebooks com atalhos direcionados aos sistemas de SP via Terminal Service para ser utilizado até que os problemas sejam sanados. Os notebooks utilizarão conexão 3G e a conexão nas dependências do ponto de encontro, RJ e SP.

Em fevereiro de 2013 foi adquirida uma nova central telefônica que comporta 2 links de voz ISDN, ou seja, podemos assim utilizar duas operadores diferentes. Assim com o canal de voz, 2 links de dados estão a disponíveis trabalhando de forma automática.

8. PLANO DE CONTINGENCIA

Os dados gerais contidos nos planos de contingências compreendem as informações apresentadas nos tópicos a seguir.

É importante que os planos de contingência sejam tempestivamente revisados, no mínimo semestralmente para assegurar a efetividade desse instrumento.

Responsáveis pela execução:

- Maurício Costa – Diretor responsável
- Ricardo Cardoso - TI Rio de Janeiro
- Oscar de Andrade - TI São Paulo

Outros funcionários e ou colaboradores envolvidos:

- Erivelto Ferreira Batista - Gerente Geral
- Sidnei Ricardo - Assistente Operacional

- Cássia Santanna - Analista de Câmbio
- Rogério Rangel - Operador de Câmbio
- Marcos Venicius - Operador de Câmbio
- Cláudio Henrique - Operador de Câmbio
- Marcos Irani - Operador de Câmbio

8.1 PROBABILIDADE DE OCORRÊNCIA

Baixo nível de ocorrência pelos históricos anteriores.

8.2 POLÍTICA E PROCEDIMENTOS PARA BACKUP

O Servidores são Virtualizados, com Snapshots em caso de evento *Disaster*.

São feitos backups diários em outros servidores internos e externos no *Cloud* via *GoogleDriv*e com criptografia. Podendo ser feito *Restore* total ou parcial dos arquivos, no servidor original de destino, ou qualquer outro definido pelo setor de T.I, dependendo do tipo de ocorrência.

8.3 PROCEDIMENTOS PARA EXECUÇÃO

A Fourtrade Corretora possui como local de utilização da estrutura de contingência a sua filial em São Paulo e a Filial utiliza a estrutura da Matriz.

Ainda como opção a Fourtrade Rio de Janeiro poderá utilizar o ponto de encontro definido na Av. Presidente Vargas, 509 – 19o andar – tel. 3970-9402 Sr. Ronaldo Dias, dependências da *Worldcount*, empresa de contabilidade da Fourtrade.

A Fourtrade São Paulo poderá utilizar as dependências da ABRACAM, Rua Boa Vista, 116 – 12º andar – Centro SP.

Os contatos com os responsáveis e os funcionários e ou colaboradores envolvidos serão feitos por celular.

Com o início do sistema de mensageria foi possível unificar a base de dados em nuvem. As equipes da Matriz e filial de São Paulo passaram a trabalhar com o sistema online via HTML e SQL, podendo ser acessado até em Home Office, pelos colaboradores.

O Servidor da filial de São Paulo e da Matriz no RJ, estão configurados para espelhar todos os arquivos em um *Cloud* na Nuvem.

Se por motivo de incêndio, catástrofes na natureza ou pane de qualquer tipo, a equipe da filial de SP ou da matriz no RJ passará a utilizar os arquivos de trabalho localizados na Nuvem.

8.4 ESTRUTURA DE SUPORTE

Em caso de efetiva necessidade de utilização da estrutura de contingência, deverão ser encaminhadas para o local as pessoas responsáveis pela tecnologia de informação, o responsável para comunicar aos diretores e os responsáveis para comunicar aos clientes.

Em caso de impossibilidade de entrar no prédio, os operadores de câmbio responsáveis pelos seus clientes ficarão encarregados de avisá-los. Caso a central não seja afetada, o mantenedor do sistema fará a transferência do link para tocar na Filial de São Paulo, assim nenhuns dos nossos clientes ficarão sem atendimento.

8.5 TESTE

Semestralmente serão avaliados os computadores e os notebooks alocados na estrutura de contingência para verificação da sua usabilidade. Se confirmado algum problema, este é prontamente resolvido para não impedir a utilização.

9. PLANO DE AÇÃO E DE RESPOSTA À INCIDENTE

Visando a implementação da prática da política de Segurança Cibernética, a Fourtrade Corretora de Câmbio definiu que o Plano de Ação e de resposta a incidentes deve abranger:

- 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; e
- Área responsável pelo registro e controle dos efeitos de incidentes relevantes.

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

9.1 RELATÓRIO

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

O 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; e
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

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 e diretoria.

10. OUTRAS INFORMAÇÕES SUJEITAS À POLÍTICA

Estão sujeitas à esta Política:

Todas as informações fornecidas ou coletadas no contexto da prestação dos serviços pela Corretora aos seus clientes para a realização das operações de Câmbio, compreendendo a captura, processamento das informações e liquidação das operações, bem como a oferta de outros serviços e produtos correlatos;

Todas as informações de funcionários, colaboradores, parceiros, terceiros, prestadores de serviço e/ou fornecedores coletadas no contexto de obrigação contratual ou legal.

Quanto à sua natureza, as informações são classificadas das seguintes formas:

Informações fornecidas pelo titular do dado:

São aquelas encaminhadas pelo titular do dado ou seu representante legal, decorrentes do cadastro junto à Corretora, como: nome completo, CPF, data de nascimento, endereço completo, dados bancários, endereço de e-mail e número de telefone.

As práticas de privacidade específicas em relação a outros produtos e serviços que a Corretora vier a disponibilizar aos seus clientes estarão associadas à aceitação pelo cliente ou terceiro de cada produto ou serviço.

11. DADOS COLETADOS, FORMA E FINALIDADE

As informações serão coletadas por meios éticos e legais e armazenadas em ambiente seguro e controlado, pelo prazo exigido na regulamentação vigente pelos órgãos reguladores. A Corretora se compromete a tomar todas as medidas cabíveis para manter o absoluto sigilo e a estrita confidencialidade de todas as informações, dados pessoais ou especificações a que tiver acesso ou que porventura venha a conhecer ou ter ciência.

O acesso de terceiros às informações coletadas pela Corretora se dá exclusivamente para atendimento das finalidades informadas nesta Política e dentro do limite necessário ao desempenho das atividades relativas ao curso normal dos seus negócios, limitando:

Bancos Parceiros de CCME (Conta Corrente em Moeda Estrangeira);

Prestadoras de serviços que executam os pagamentos SPB (liquidações das operações) das operações;

Prestadores de serviços que utilização armazenamento em nuvem de informações de clientes;

Parceiros de Marketing;

Auditores independentes;

Órgãos reguladores competentes.

A utilização das informações coletadas pela Corretora, em qualquer das hipóteses previstas acima, é feita exclusivamente para atendimento das finalidades informadas nesta Política no desempenho das atividades da Corretora.

A Corretora poderá compartilhar informações de forma agregada com os seus Correspondentes Cambiais e/ou com seus parceiros mediante autorização do proprietário dos dados. Esta autorização poderá ser coletada na ficha cadastral PF ou PJ.

12. SEGURANÇA DAS INFORMAÇÕES

Visando a segurança das informações fornecidas pelos clientes, a Corretora dispõe de processos de segurança físicos, lógicos, técnicos e administrativos compatíveis com a sensibilidade das informações coletadas, cuja eficiência é periodicamente avaliada por auditoria independente e testes de contingências.

A Corretora implementa novos procedimentos e melhorias tecnológicas contínuas para proteger todos os dados pessoais coletados dos clientes.

Não obstante as medidas de segurança adotadas, a Corretora não se responsabiliza por prejuízos decorrentes da violação da confidencialidade das informações em virtude da ocorrência de qualquer fato ou situação que não lhe seja imputável.

No tratamento das informações coletadas, a Corretora utiliza de sistemas estruturados de forma a atender aos requisitos de segurança e transparência, aos padrões de boas práticas e de governança e aos princípios gerais estabelecidos na Lei nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais (“LGPD”).

Para garantir que as informações de negócios e os dados dos clientes sejam tratados com o devido cuidado, a Fourtrade, assim como qualquer colaborador que lida com esses dados, utilizará exclusivamente canais oficiais da própria instituição em conformidade com a LGPD. De preferência é do e-mail, mas quando não for possível, é permitido usar o telefone corporativo ou aplicativo de mensagens ligado a este. Portanto, o uso de ferramentas pessoais, incluindo o contato com clientes externos e a transmissão de documentos online, não será permitido e deve ser evitado.

Todas as tecnologias utilizadas respeitarão sempre a legislação vigente e os termos desta Política.

13. APROVAÇÃO, REVISÃO E DIVULGAÇÃO DA POLÍTICA

Esta Política está aprovada pela Diretoria, registrada em Ata de Reunião de Diretoria e está sendo publicada e comunicada para todos os funcionários e partes externas relevantes para o necessário cumprimento.

A Política será revisada criticamente em periodicidade anual ou quando observadas mudanças relevantes na atuação da Instituição.

14. BASE NORMATIVA

RESOLUÇÃO CMN Nº 4.893, DE 26 DE FEVEREIRO DE 2021 - Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 – Lei Geral de Proteção de Dados (LGPD).

LEI COMPLEMENTAR Nº 105, DE 10 DE JANEIRO DE 2001 - Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.