POLÍTICA DE SEGURANÇA

CIBERNÉTICA DA

ARC CORRETORA DE CÂMBIO

ÍNDICE

1. OBJETIVO

Este normativo estabelece a Política de Segurança Cibernética da **ARC Corretora de Câmbio** visando total observância e adequação ao exigido na Resolução Bacen nº 4.893 de 26 de fevereiro de 2.021.

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.

O resumo desta Política está sendo divulgado ao público geral, especialmente clientes, parceiros, prestadores de serviços, administradores e colaboradores.

2. PORTE, RISCO E MODELO DE NEGÓCIO

A ARC Corretora de Câmbio é uma instituição de pequeno porte, que se dedica a efetuar operações de câmbio em espécie, cartões pré-pagos, remessas através de Bancos parceiros e intermediação de importação e exportação, apresentando risco operacional de nível baixo e pouca exposição cambial. Seus negócios se dão por acesso dos clientes à sede da instituição, à Rua do comércio. 55 – 7 andar, Conj. 74, Santos, SP.

3. NATUREZA DAS OPERAÇÕES E COMPLEXIDADE DOS PRODUTOS

Nossas operações são presencias na sede. São operações de câmbio manual de compra e venda de moeda estrangeira, remessas e prestação de serviço nas operações de importação e exportação, sendo a operação cambial efetuada por Bancos autorizados e Bancos parceiros. Tanto as operações como a prestação de serviço se referem a elementos de pouca complexidade, não deixando de considerar a responsabilidade à política de segurança cibernética e a prevenção à lavagem de dinheiro e o combate de financiamento do terrorismo.

4. CONCEITOS

Confidencialidade: é a garantia de que as informações sejam acessadas somente por pessoas autorizadas.

Integridade: é a garantia de preservação da precisão, consistência e confiabilidade das informações e sistemas pela empresa ao longo dos processos ou de seu ciclo de vida.

Disponibilidade: é garantir que as informações e os recursos estejam disponíveis para aqueles que precisam deles quando necessário.

Ameaças e riscos cibernéticos

Os avanços tecnológicos e a internet criam facilidades e possibilitam o uso de várias ferramentas para a atuação das Instituições Financeiras, trazendo agilidade na execução e disponibilização de serviços.

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

São várias as razões que levam os hackers a realizar esses ataques, por exemplo:

- Manipulação ou adulteração de informações e ganhos financeiros através de contas bancarias e o uso de cartão crédito das vítimas;
- Obter informações confidenciais de Instituições e clientes, visando a concorrência;
- Expor a Instituição invadida por motivos de vingança;
- Praticar o terror e disseminar pânico e caos.

Os hackers se utilizam de vários métodos para os ataques cibernéticos, segue alguns exemplos:

- **Vírus:** software que causa danos a máquina, rede, softwares e banco de dados;
- **Malware:** softwares desenvolvidos para corromper computadores e redes:
- **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.
- **Cavalo de Troia:** aparece dentro de outro software e cria uma porta para a invasão do computador;
- **Engenharia social:** métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
- **Pharming:** manipulação para direcionar usuários para sites falsos, que vão instalar softwares maliciosos nos computadores dos visitantes ou coletar dados pessoais;
- **Phishing:** links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- **Vishing:** simulação de uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta persuadir a vítima a fornecer informações confidenciais;
- **Smishing:** simulação de uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta persuadir a vítima a fornecer informações confidenciais;
- **Ataques de DDoS** (Distributed denial of services): Ao realizar um chamado ataque de negação de serviço, os criminosos enviam inúmeros pedidos de acesso simultaneamente para esgotar a capacidade de resposta de um provedor e torná-lo indisponível.
- **Botnets**, vários computadores infectados e controlados remotamente por hackers para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

5. ÁREA GESTORA DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Responsável: Mauricio Sinigoi Campos

Atribuições:
– Responsável pela Política de Segurança Cibernética
– Responsável pela execução do Plano de Ação e de resposta a incidentes

6. PROCEDIMENTOS E CONTROLES ADOTADOS PARA MITIGAR A VULNERABILIDADE DA INSTITUIÇÃO

Atualmente a ARC corretora faz uso de ferramentas de bloqueio dos diversos e mais recentes tipos de ameaças, bloqueio de portas e IP's, aplicativos com códigos maliciosos, scripts, arquivos bat, conexões, bloqueio por analise comportamental e reputação, lista de controle de acesso (ACL), atualização de senhas. A fim de atender e se adequar à Política de Segurança Cibernética, conforme resolução nº 4.893 de 25 de fevereiro de 2.021 do Banco Central do Brasil, a ARC Corretora irá contratar ferramentas e serviços de prevenção de vazamento de informações, realização de testes e varreduras para detecção de vulnerabilidade, mecanismos de rastreabilidade, incluindo trilhas de auditoria, gerenciamento de logs, etc.

6.1. TREINAMENTO DO PESSOAL E CAPACITAÇÃO

Conscientização e orientação via e-mail de melhores práticas de segurança para utilização dos sistemas da corretora, como:

- Alertas sobre e-mail's maliciosos que contenham links e anexos;
- A estarem atentos sobre os alertas do antivírus, principalmente no que diz respeito a possíveis tentativas de intrusão e atualização do antivírus;
- A desconfiar de sites que o antivírus alertou como não seguro, mesmo que o site tenha o cadeado seguido do protocolo **https,** que garante a conexão entre usuário e o site seja criptografada torando-a mais segura, é preciso estar atento ao certificado digital no que diz respeito a sua validade e autenticidade, verificar o nome do site se está correto ou qualquer outra coisa que desconfie;
- Divulgação de normas relacionadas à Politica de Segurança Cibernética.
- Cursos de capacitação em segurança cibernética.

6.2. LOGIN E SENHA

- As senhas para acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário do 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, data de nascimento e não devem ser constituídas de forma sequencial como "abcd", "1234", entre outras.
- Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

6.3. SITE

- O site da ARC Corretora tem como objetivo informar ao internauta/cliente sobre os seus serviços prestados e através do QUERO COTAR, simplesmente garantir a taxa de compra ou venda e iniciar um contato com a corretora através de telefone e e-mail.
- O site da ARC Corretora possui protocolo de segurança que garante que os dados do cliente sejam transmitidos de forma segura por meio de uma conexão criptografada.
- O Site da ARC Corretora não pede nenhuma informação além do valor a ser cotado, nome e telefone. Outras informações necessárias serão solicitadas através do nosso e-mail.
- A ARC Corretora recomenda não utilizar Lan house ou computares não confiáveis para fazer compras ou transações financeiras.
- Mesmo usando o computador de casa ou do trabalho, é importante ficar atento ao domínio (endereço de internet) do site que está sendo acessado, verifique se o site confiável.

6.4. ATUALIZAÇÃO DO SISTEMA E INSTALAÇÃO DE PROGRAMAS

- Qualquer manipulação da base de dados, atualização ou upgrade realizado pela empresa responsável pelo sistema de câmbio deve ser agendado de forma que possa ser assistido pelo técnico de TI dessa corretora, respeitando as políticas de segurança.
- 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.
- Fazer testes de continuidade dos negócios em caso de incidente

7. PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Em caso de ocorrência de um incidente cibernético ou indisponibilidade de recursos computacionais, serão tomadas todas as medidas possíveis para analisar e corrigir a falha, fazer o registro, a análise da causa e do impacto e dar continuidade aos negócios sem que haja prejuízo para corretora e seus clientes.

7.1. 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
- vazamento de dados/ informações
- Indisponibilidade de acesso à Corretora

- Indisponibilidade de recursos computacionais
- 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 estará avaliando 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 por ventura 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.

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.

7.2. COMUNICAÇÃO AO BANCO CENTRAL DAS OCORRÊNCIAS DE INCIDENTES

A **ARC Corretora de Câmbio** deverá informar ao Banco Central do Brasil as ocorrências de incidentes relevantes e as interrupções dos serviços relevantes que configurem uma situação de crise,

Essa comunicação deve ser acompanhada das informações sobre o incidente ocorrido bem como das informações sobre as providências tomadas para o reinício das atividades.

8. REGULAMENTAÇÃO ASSOCIADA

Resolução Bacen nº 4.893 de 26 de fevereiro de 2.021 (revoga a Resolução Bacen nº 4.658 de 26 de abril de 2.018 e a Resolução nº 4.752 de 26/09/2019).

Circular Bacen nº 3.909, de 16 de agosto de 2.018