POLÍTICA DE SEGURANÇA CIBERNÉTICA

Esta política foi elaborada para atender aos requisitos e diretrizes da Resolução CMN 4.893 de 26/02/2021 e a Resolução BCB 85 de 08/04/2021.

A presente política abrange os aspectos relativos à segurança da informação e controles sobre Riscos Cibernéticos, envolvendo tecnologias, processos, pessoas e instalações físicas, sendo aplicada a todas as áreas, colaboradores e prestadores de serviço da Singratur Corretora de Câmbio Ltda.

1. Objetivo

Esta política tem como objetivo estabelecer as diretrizes necessárias para assegurar a confidencialidade, a integridade, a segurança e a disponibilidade dos dados e dos sistemas de informação utilizados pela Singratur Corretora de Câmbio Ltda, além de direcionar um programa efetivo de prevenção, detecção e redução de impactos gerados pelos incidentes relacionados ao ambiente cibernético, em conformidade com as melhores práticas de mercado e legislação aplicada. Dessa forma, a política busca mitigar riscos cibernéticos, proteger os dados dos clientes, garantir a continuidade dos serviços e promover a confiança no ambiente financeiro.

É objetivo desta política, ademais, estabelecer plano de ação e de resposta a incidentes visando, além da implementação da política de segurança cibernética, à:

a) Proteger o valor e a reputação da empresa;

b) Garantir a confidencialidade, integridade e disponibilidade das informações da Singratur, e de informações de terceiros por ela custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

c) Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;

d) Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

e) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes à atividade da empresa;

f) Conscientizar, educar e treinar os colaboradores por meio de Política de Segurança Cibernética, normas e procedimentos internos aplicáveis às suas atividades diárias;

g) Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

2. Governança

A elaboração, manutenção e a disponibilização desta Política são de responsabilidade da Diretoria de Segurança Cibernética e das gerências Operacional e Administrativa da Singratur Corretora de Câmbio.

Todos os colaboradores da Singratur são responsáveis pela assimilação, incorporação no seu dia-a-dia e na manutenção da Segurança Cibernética em todos os processos, tanto nas suas próprias atividades como no relacionamento com outros colaboradores e com agentes externos à Corretora.

O Diretor de Segurança Cibernética é o responsável por acionar auxílio técnico quando necessário, para qualquer evento envolvendo computadores, servidor, backup ou outro evento cibernético relevante na Singratur.

O Diretor de Segurança Cibernética está devidamente cadastrado no Unicad.

3. Definições e Conceitos

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Confidencialidade: garantia de que a informação é acessível somente às pessoas autorizadas.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento. Confiabilidade das informações.

Disponibilidade: garantia de que os usuários ou processos autorizados obtenham acesso à informação e aos recursos associados correspondentes sempre que necessário.

Backup ou Salvaguarda: Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada.

Colaborador: Empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente com a Singratur.

Informação: É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

Internet: Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente.

Recursos de Tecnologia da Informação e Comunicação: hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

Segurança da informação: É a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

Risco: Combinação dos impactos advindos da ocorrência de um evento indesejado relacionado à segurança da informação e da probabilidade de sua ocorrência.

Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets, ransomware), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Malwares:

- 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:

- 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.

Fraudes Externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

Ataques DDoS 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 enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à

Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

4. Princípios da Segurança Cibernética

Os princípios básicos da segurança cibernética são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

- **Confidencialidade:** Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.
- **Integridade:** Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.
- **Disponibilidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.
- **Acesso controlado:** O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. A ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

5. Diretrizes Corporativas

O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
- Assegurar que os recursos utilizados para o desempenho das funções de cada colaborador sejam utilizados apenas para as finalidades de negócios da Singratur Corretora de Câmbio Ltda;
- Garantir que os sistemas e as informações sob a responsabilidade de cada colaborador estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Atender às leis que regulamentam às atividades da Singratur Corretora de Câmbio Ltda e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Comunicar imediatamente à área de Segurança Cibernética, quaisquer descumprimentos da Política de Segurança Cibernética.

6. Tratamento de Incidentes

Os incidentes identificados devem ser reportados ao Diretor de Segurança Cibernética da Singratur, por qualquer colaborador, que deverá mencionar o tipo do incidente ocorrido, conforme detalhado abaixo, mas não se limitando a tais:

- Falha de Segurança Cibernética/Informação: informações sensíveis/confidenciais disponíveis sem restrição; compartilhamento de senhas; acesso não autorizado, ataque cibernético, malwares, etc.;
- Falha ou Erro em sistemas: sistema com mensagem de erro; sistema realizando cálculo errado, sistema travado, etc.;
- Indisponibilidade: queda de link de internet; linha telefônica indisponível; falta de energia elétrica, etc.;
- Lentidão: rede, banco de dados, sistemas apresentando lentidão excessiva, etc.;

- Falha Operacional: processo não executado da forma correta e/ou definida, etc.;
- Fraudes: operações atípicas que denotam fraudes.

A comunicação do incidente pode ser realizada pessoalmente, na sede da Singratur, por meio telefônico, falado ou escrito (e-mail, Whatsapp). O relato do evento (incidente) deve ser bem detalhado a fim de prover informações suficientes para as devidas tratativas.

Anualmente, com data-base em 31/12, deve ser emitido o relatório sobre o gerenciamento de incidentes do período, com a disponibilização ao Órgão Regulador.

7. Continuidade dos Negócios

O processo de gestão de continuidade de negócios, relativo à segurança da informação, deve ser implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

8. Armazenamento de Backup em Nuvem

Conforme a Resolução CMN n° 4.893 e Resolução 85 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Singratur mantém um procedimento efetivo que assegure a aderência às regras previstas na regulamentação em vigor.

Para os fins de aderência regulatória sobre a análise de riscos operacionais e cibernéticos, de continuidade de negócios, de confidencialidade, de disponibilização de informações ao Órgão Regulador, de Resposta a Incidentes, dentre outros, deve-se contemplar o processo de due-diligence junto ao fornecedor do produto ou serviço contratado, previamente à formalização do contrato de prestação de serviços entre a contratante (Singratur) e a contratada (Fornecedor).

O processo de due-diligence engloba a pesquisa de reputação da empresa a ser contratada, a solicitação de especificações técnicas referente ao produto ou serviço a ser contratado, a verificação sobre certificações de segurança da empresa e a verificação sobre o atendimento às normas da LGPD. É verificado também sobre a empresa realizar a criptografia dos dados e sobre registros de auditoria.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, bem como as alterações contratuais desses serviços, devem ser comunicadas ao Banco Central do Brasil, até dez dias após a contratação dos serviços ou das alterações contratuais.

9. Conscientização dos Funcionários e Parceiros

O diretor de Segurança Cibernética realiza reuniões informais na sede da Singratur, sobre a conscientização de segurança da informação e riscos cibernéticos, com a participação dos funcionários e eventuais parceiros e prestadores de serviços.

Esta política também é divulgada no site da Singratur, para que os funcionários e parceiros se familiarizem com as diretrizes e os procedimentos da Singratur.

10. Violações à Política

São consideradas violações à Política de Segurança Cibernética e às respectivas normativas, as seguintes situações, não se limitando a estas:

- Quaisquer ações ou situações que possam expor a Singratur à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- Uso indevido de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Diretor de Segurança Cibernética;
- Uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da Singratur;
- A não-comunicação imediata à área de Segurança Cibernética sobre quaisquer descumprimentos da Política.

Indícios de irregularidades no cumprimento das determinações desta política devem ser comunicadas imediatamente para o Diretor de Segurança Cibernética, de forma escrita ou falada.

11. Aprovação e Atualizações

Esta política foi revisada e aprovada pelo Diretor de Segurança Cibernética na reunião n° 27 em 31/03/2025.

Revisões e atualizações subsequentes devem ocorrer anualmente ou de acordo com revisões de processo ou ajustes para cumprir com requisitos legais ou regulatórios.

_____

Alberto Haddad

Diretor de Segurança Cibernética