POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. DEFINIÇÃO

O termo INSTITUIÇÃO, citado ao longo deste documento, refere-se indistintamente à CODEPE Corretora de Valores e Câmbio S/A e/ou Ótimo Sociedade de Crédito Direto S/A, quando aplicável.

O termo CORRETORA faz referência exclusivamente à CODEPE Corretora de Valores e Câmbio S/A, o termo ÓTIMO faz referência exclusivamente a ÓTIMO Sociedade de Crédito Direto S/A.

2. OBJETIVO

A Política de Segurança Cibernética tem como objetivo definir diretrizes, princípios, regras e procedimentos referente às melhores práticas, visando assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados na INSTITUIÇÃO.

3. DIRETRIZES

Para o cumprimento da presente Política, a INSTITUIÇÃO definiu as diretrizes a seguir, que deverão ser respeitadas por todos os colaboradores, terceiros e parceiros comerciais:

(a) Proteger e gerenciar dados, informações e acessos, a fim de garantir a confidencialidade, integridade e disponibilidade;
(b) Promover a segurança física e lógica, com o controle de acesso e proteção das ameaças físicas e ambientais;
(c) Classificar as informações, por meio do tratamento e requisitos de segurança, conforme importância dos dados e sistemas de processamento;
(d) Gerenciar os acessos às informações, com a definição de níveis de acesso e segregação de funções;
(e) Definir o plano de ação para resposta a incidentes de segurança cibernética;
(f) Conscientizar e treinar todos os colaboradores em segurança da informação;
(g) Garantir a continuidade de negócios e proteção das informações críticas;
(h) Gerenciar o processo de continuidade de negócios relativo à segurança da informação;
(i) Avaliar as ameaças e riscos na contratação de serviços e fornecedores;
(j) Executar plano de continuidade de negócios visando prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
(k) Atender a legislação vigente e seu mercado de atuação.

A INSTITUIÇÃO criou mecanismos para disseminar a cultura de segurança cibernética com a implementação do programa de Conscientização de Segurança da Informação.

A INSTITUIÇÃO disponibiliza na sua página oficial na internet as principais recomendações de segurança na utilização dos produtos e serviços financeiros aos seus clientes e usuários.

4. TRATAMENTO DE INCIDENTES

4.1 A área de Tecnologia da Informação gerencia o registro de incidentes, com análise da causa e do impacto, bem como com o controle dos efeitos relevantes para as atividades.

5. PROCEDIMENTOS E CONTROLES

A INSTITUIÇÃO adotou procedimentos e controles para reduzir a vulnerabilidade a incidentes, como os a seguir:

- Parâmetros de senha
- Prevenção e a detecção de intrusão
- Prevenção de vazamento de informações
- Realização periódica de testes e varreduras para detecção de vulnerabilidades
- Proteção contra softwares maliciosos
- Estabelecimento de mecanismos de rastreabilidade
- Controles de acesso e de segmentação da rede de computadores
- Manutenção de cópias de segurança dos dados e das informações

6. DA DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A presente política é divulgada na intranet a todos os colaboradores da INSTITUIÇÃO, e ao público em geral, em versão simplificada, na página oficial na internet.

Para os prestadores de serviços e terceiros, cópia da política de segurança cibernética é disponibilizada.

7. DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

A INSTITUIÇÃO estabeleceu plano de ação e de resposta a incidentes visando adotar controles para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de segurança cibernética.

A INSTITUIÇÃO designou Diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

8. DA CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

8.1 A INSTITUIÇÃO assegura que suas políticas, estratégias e estruturas para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplam a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País.

8.2 A INSTITUIÇÃO, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, adotará procedimentos que contemplem:

(a) A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

(b) A verificação da capacidade do potencial prestador de serviço de assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da INSTITUIÇÃO aos dados e às informações a serem processadas ou armazenadas pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviço;
- Sua aderência às certificações exigidas pela INSTITUIÇÃO para a prestação do serviço a ser contratado;
- O acesso da INSTITUIÇÃO aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos clientes da INSTITUIÇÃO por meio de controles físicos ou lógicos; e
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da INSTITUIÇÃO.

Na avaliação da relevância do serviço a ser contratado, a INSTITUIÇÃO deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo contratado.

No caso da execução de aplicativos por meio da internet, utilizando recursos do próprio prestador de serviços, a INSTITUIÇÃO deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

A INSTITUIÇÃO deve possuir recursos e competências necessárias para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso de recursos providos para monitoramento dos serviços a serem efetuados.

Para os fins do disposto nesta Política, os serviços de computação em nuvem abrangem a disponibilidade à INSTITUIÇÃO, 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 ao contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
(b) Implantação ou execução de aplicativos desenvolvidos pela INSTITUIÇÃO, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou
(c) Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A INSTITUIÇÃO, quando contratante de serviços, será responsável pela confiabilidade, integridade, disponibilidade, segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada ao Banco Central do Brasil, devendo as informações conter:

(a) 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, no caso de contratação no exterior.

A comunicação de que trata o parágrafo anterior deve ser realizada, no mínimo, sessenta dias antes da contratação dos serviços.

As alterações contratuais que impliquem modificação das informações de que tratam os itens A, B e C acima devem ser comunicadas ao Banco Central do Brasil, no mínimo, sessenta dias antes da alteração contratual.

Os contratos para prestação 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 citados no item anterior;
(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 citados no item A ao novo prestador de serviços ou à própria INSTITUIÇÃO; e
- Exclusão dos dados citados no item acima pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;

(e) O acesso da INSTITUIÇÃO a:
- Informações fornecidas pela empresa contratada, visando verificar o cumprimento do disposto nos itens A, B e C acima;
- Informações relativas às certificações e aos relatórios de auditoria especializada;
- Informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados.

(f) A obrigação de a empresa contratada notificar a INSTITUIÇÃO sobre a subcontratação de serviços relevantes;
(g) A permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;
(h) A adoção de medidas pela INSTITUIÇÃO, em decorrência de determinação do Banco Central do Brasil; e
(i) A obrigação de a empresa contratada manter a INSTITUIÇÃO permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

O contrato deve prever:

(a) A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de

segurança dos dados e das informações, bem como aos códigos de acesso, que estejam em poder da empresa contratada; e

(b) A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

- A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e
- A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da INSTITUIÇÃO.

NOTA:

O disposto no item 8 desta Política não se aplica à contratação de sistemas operados por câmaras, por prestadores de serviços de compensação e de liquidação ou por entidades que exerçam atividades de registro ou de depósito centralizado.

9. DISPOSIÇÕES GERAIS

A INSTITUIÇÃO instituiu, através desta Política, 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, incluindo:

(a) A definição de processos, testes e trilhas de auditoria;
(b) A definição de métricas e indicadores adequados; e
(c) A identificação e a correção de eventuais deficiências.

10. DISPOSIÇÕES FINAIS

Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

(a) Esta política de segurança cibernética;
(b) O documento relativo ao plano de ação e de resposta a incidentes;
(c) O relatório anual;
(d) Os contratos a partir do prazo da extinção do contrato; e
(e) Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle, contado o prazo a partir da implementação dos citados mecanismos.

11. APROVAÇÃO, VIGÊNCIA E REVISÃO

A Diretoria é responsável pela aprovação desta Política, devendo também supervisionar e controlar seu cumprimento e os processos a ela relacionados.

Esta Política entra em vigor na data de sua publicação e deve ser revisada, no mínimo, anualmente ou imediatamente, caso seu conteúdo sofra alguma alteração.

REFERÊNCIAS REGULATÓRIAS

BRASIL. Resolução Banco Central nº 4.658, de 26 de abril de 2018.