Política de Segurança Cibernética

Introdução.

Esta política foi formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

A política está compatível com:

I- O porte, o perfil de risco e o modelo de negocio da instituição financeira não bancária.
II- A natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e
III- A sensibilidade dos dados e das informações sob responsabilidade da instituição.

Objetivo:

O principal objetivo da segurança da informação é proteger os dados e não somente os ativos físicos e tecnológicos por onde eles passam ou estão armazenados. A partir dessa premissa, existe uma independência nos conceitos da informação em relação à tecnologia.

Para esclarecimento iremos citar três pontos chaves, envolvidos:

Confidencialidade: este é um ponto estratégico para toda e qualquer empresa. A cooperativa está situada dentro da empresa mantenedora Astrazeneca e atendemos somente a funcionários com prazo indeterminado, sendo assim a confidencialidade nos dados pessoais e/ou gerencias é de suma importância.

Integridade: nos indica que toda a informação seja armazenada e transferida corretamente para quem a consulta, isto é, assegurar a sua exatidão, além de assegurar também que os métodos de processamento estejam corretos. Operacionalmente, a integridade da informação valida todo o processo de comunicação dentro e fora da instituição.

Disponibilidade: este fator está mais envolvido com a rotina operacional da instituição.

A instituição contratante é responsável pela confiabilidade, integridade, disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como o cumprimento da legislação e da regulamentação em vigor.

Com base na resolução de nº 4658, Art 2º parágrafo 1º inciso I:

A Cooperativa dos Funcionários da Astrazeneca está enquadrada no porte de Singular S5, onde o nível de risco é considerado baixo e temos como modelo de negocio o cooperativismo de capital e emprestimo com consignado em folha.

Política de Segurança Cibernética

Inciso II:
Natureza das operações: as operações de capital e empréstimo são oriundas de funcionários da empresa mantenedora.

Complexibilidade dos produtos, serviços, atividades e processos da instituição: Os valores referentes ao capital e parcelas de empréstimos contratados são descontados na folha de pagamento conforme *política de crédito vigente e manual operacional de segurança cibernética.*

Sensibilidade dos dados e das informações da instituição: A cooperativa transita somente dados pessoais.

"Dados Pessoais" significa quaisquer informações relacionadas a pessoa natural identificada ou identificável, por exemplo: nome, sobrenome, idade, endereço residencial, e-mail, RG, CPF/ME, dados de localização (GPS ou WiFi), número do *Internet Protocol* (IP).

"Dados Pessoais Sensíveis" significa qualquer dado pessoal que seja referente à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. A título de exemplo, podem ser elencados como Dados Pessoais Sensíveis aqueles coletados durante a inscrição ou prestação de serviços de saúde, informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, dados genéticos, dados biométricos, amostras biológicas, dados sobre doenças, dados sobres deficiência, dados sobre risco de doença, histórico clínico, tratamento clínico e prontuários.

Procedimentos e controles

Visando atender a Seção I do Art.3º Inciso I ao V, alíneas de A até D , inciso VI e alíneas de A até C, inciso VII ,§ 1º ao 5º e seção III art.6º ao art.10 será possível identificar *no manual de Segurança Cibernética Coopaz* o detalhamento dos procedimentos, controles específicos, registros de análise e causa do impacto, compartilhamento de informações e diretrizes adotadas para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética.

Da contratação de serviços de processamento e armazenamento de dados e de computação em nuvem

A instituição singular (S5) Coopaz, assegura que suas políticas, estratégicas 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.

Política de Segurança Cibernética

Sendo assim, adotamos procedimentos que contemplam, quanto á:

a) A adoção de práticas de governança corporativa e de gestão proporcionais a 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;

c) O cumprimento da legislação e regulamentação em vigor;

d) O acesso da instituição aos dados e as informações a serem processados ou armazenados pelo prestador de serviço;

e) A confiabilidade, a integridade, a disponibilidade e a recuperação dos dados e as informações ou armazenamentos pelo prestador de serviço;

f) A aderência a certificações exigidas pela instituição para a prestação de serviço a ser contratado;

g) O acesso da instituição contratante aos relatórios por empresa de auditoria especializada independente, por ela contratada;

h) Informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

i) A identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

j) A qualidade dos controles de acesso voltados a proteção dos dados e das informações dos clientes da instituição.

Rodovia Raposo Tavares, KM 26,9- Cotia/SP- CEP: 06707-000.
Tel.11 37371261 ou 11 37374516 e-mail: coopaz@astrazeneca.com

Política de Segurança Cibernética

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 gerenciados pelo contratado, levando em conta, inclusive, a classificação das diretrizes de relevância.

Deve-se documentar os procedimentos referentes a verificação.

A instituição deve assegurar que o potencial prestador de serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades nas liberações de novas versões do aplicativo.

Os serviços de computação em nuvem abrangem a disponibilidade 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 instituição implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos.

Os computadores e rede utilizada é da empresa mantenedora Astrazeneca do Brasil, onde seguimos a *Política Global de uso da tecnoligia da informação corporativa.*

Em caso de contratação ou alteração contratual de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada pela instituição com no mínimo 60 dias antes da contratação, ao Banco Central.

Na comunicação deve constar a denominação da empresa a ser contratada, os serviços relevantes e indicação de países e regiões em caso de contratação no exterior.

Disposições Gerais

A instituição assegura que a politica de gerenciamento de risco prevista na regulamentação em vigor, dispõem no tocante a continuidade do negócio, sobre:

Tratamento dos incidentes relevantes relacionados com o ambiente cibernético e procedimentos para mitigar.

Procedimentos e prazos a serem cumpridos no caso de interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo

cenários que considerem a substituição da empresa contratada e reestabelecimento da operação normal da instituição.

Cenários de testes de continuidade de negócio e a comunicação tempestiva ao banco Central do Brasil das ocorrências relevantes que configurem uma situação de crise pela instituição financeira não bancária, bem como as providencias para o reinicio das suas atividades.

Fica determinado o acompanhamento e controle com vistas a assegurar a implementação e a efetividade da politica 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 métrica e indicadores adequados; e
c) Identificação e a correção de eventuais deficiências.

Disposições Finais

A Instituição deve deixar disponível pelo prazo de cinco anos, para o Banco Central do Brasil os seguintes documentos:

1. Política da Segurança Cibernética;
2. A ata de reunião do conselho de administração ou, na sua inexistência, da Diretoria Executiva;
3. O Plano de ação e de Respostas a incidentes;
4. O relatório anual de implementação do plano de ação e de respostas a incidentes;
5. A documentação sobre os procedimentos a verificação da capacidade do potencial prestador de serviço.

A política Cibernética, o Plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente. Conforme prevê a Resolução nº 4.658.

Política aprovada em 18 de setembro de 2019, em reunião extraordinária da Diretoria Executiva.

Vanessa Tedeschi Cordaro Levy
Diretora Presidente

Mariana Campanate Rodrigues Viñau
Diretora Secretária