SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA – PO-013

POLÍTICA

1. INTRODUÇÃO

Na política de segurança da informação e cibernética serão demonstradas as premissas que visam garantir a aplicação de princípios e diretrizes das informações organizacional e dos clientes, permitindo fornecer parâmetros gerais às atividades de proteção de ativos e gestão de informações relevantes ao Banco Arbi S.A e seus clientes.
A política está em conformidade com a Resolução 4.658 de 26.04.2018 do Banco Central do Brasil e suas atualizações.

2. OBJETIVO

Estabelecer as diretrizes e princípios que busquem assegurar a proteção a ativos e informações disponíveis no Banco Arbi, própria e de terceiros, visando minimizar impactos sobre as atividades operacionais, e contingenciá-los quando possível.

3. PRINCÍPIOS

O Banco Arbi S.A utilizará como referência em suas atividades de segurança da informação e cibernética, os princípios conforme descritos abaixo:

Compatibilidade de porte, perfil e modelo de negócio da instituição;

Natureza das operações e **complexidade dos produtos**, serviços, atividades e processos desenvolvidos pela instituição;

Sensibilidade dos dados e informações recebidas, armazenadas e transferidas, diante de autorização prévia;

Disponibilidade de dados e informações, de forma a garantir o uso por pessoas autorizadas a fazê-lo;

Integridade de dados e informações, garantindo a exatidão da coleta, processamento, uso e guarda dos mesmos.

Confidencialidade de dados e informações, mantidas a reserva de acesso ao que por autorização ou função tenham o direito de uso.

Vulnerabilidade de dados e informações, implementar ferramentas, processos e controles para a minimização dos riscos.

Rastreabilidade de dados, informações e acessos para identificar e controlar a segurança dos sistemas de informações da instituição.

4. DIRETRIZES

O Banco Arbi S.A utilizará como referência em suas atividades de segurança da informação e cibernética, as diretrizes conforme descritas abaixo:

As informações e dados próprios e de terceiros devem ser tratadas de forma ética, sigilosa e de acordo com as leis vigentes e normas internas, evitando o mau uso e exposição indevida;

O acesso às informações e recursos deverá ser realizado se devidamente autorizado para fazê-lo;

A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável por suas ações realizadas;

A concessão de acessos obedecerá ao critério de menor privilégio, no qual o usuário terá acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

A senha deverá ser utilizada com assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;

Os riscos identificados de ativos, informações e dados devem ser reportados à área de Compliance e Controles Internos;

As responsabilidades quanto à segurança da informação e cibernética devem ser divulgadas aos colaboradores, que devem entender e assegurar o cumprimento das diretrizes descritas.

5. CLASSIFICAÇÃO DAS INFORMAÇÕES

O Banco Arbi utiliza as seguintes categorias para efeitos de classificação da informação:

- Uso público
- Uso restrito interno por departamento
- Uso confidencial

Todos os dados e informações são classificados em função de sua sensibilidade, criticidade e propósito. Os dados e informações são armazenados em sistemas seguros, com controle de acesso adequado ao perfil de cada usuário

6. TRATAMENTO DOS DADOS E DAS INFORMAÇÕES

O Banco Arbi S.A visando oferecer a proteção adequada em observância aos princípios e diretrizes descritos, os dados e informações adotaram os seguintes processos:

GESTÃO DE ATIVOS DA INFORMAÇÃO: Está baseado em tudo o que pode criar, processar, armazenar, alterar, transmitir ou até excluir informações. Podendo ser tecnológico ("software" e "hardware") e não tecnológico (pessoas e processos);

TRANSMISSÃO DE DADOS: A instituição utilizará meios que garantam a transmissão de dados com segurança e sigilo, podendo se valer de criptografias e outras tecnologias disponíveis para tal.

CLASSIFICAÇÃO DE DADOS E INFORMAÇÕES: Estarão classificadas conforme sua confidencialidade e Relevância, em Restrito, Confidencial, Interna e Pública e para tanto deverão ter acessos e proteção adequados as suas classificações;

GESTÃO DE ACESSOS: As concessões, revisões e exclusões de acesso devem utilizar como referência o Status (Inabilitado, Ativo e Inativo), Perfil (Administrador ou Master, Usuários e suas subdivisões) dado ao colaborador e a autorização para tal;

GESTÃO DE RISCOS: Os sistemas de informações devem focar minimamente nos critérios de identificação de Vulnerabilidade, Ameaças e Impactos, para que sejam recomendadas as proteções adequadas.

CENÁRIOS DE RISCOS: Constará no Plano de Continuidade de Negócios, sendo o fórum apropriado, os cenários de riscos testados para continuidade dos negócios;

CLASSIFICAÇÃO DOS INCIDENTES CIBERNÉTICOS: Estarão classificadas conforme seu impacto operacional e financeiro, em Pontual, Baixo, Médio, Relevantes e Critico e em conformidade com seu impacto

proceder prazos máximos para o restabelecimento a normalidade das atividades;

TRATAMENTO DE INCIDENTES: A ocorrência de incidentes, devem ser reportados ao Compliance e Controles Internos, para a adoção de procedimentos e manutenção dos registros;

COMPARTILHAMENTO DE INFORMAÇÕES DE INCIDENTES: Sempre que viável, seguro, integro e disponível, de forma a ajudar a ampliar os controles de incidentes, a instituição poderá fornecer ou receber informações de incidentes ocorridos. Diante de autorização prévia dos representantes de cada instituição ou para associações de representação.

GOVERNANÇA DE NEGÓCIOS E TECNOLOGIA: Todas as iniciativas e projetos devem preservar os princípios e diretrizes constantes nesta política, garantindo a Sensibilidade, Disponibilidade, Integridade e Confidencialidade.

SEGURANÇA FÍSICA DO AMBIENTE: O acesso físico à ambientes que realizem a recepção, processamento, emissão e guarda de informações deverá apresentar distinção de acesso para pessoas autorizadas, conforme o perfil do colaborador.

PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES: A formalização do plano de ação e de resposta a incidentes deverá elencar a adequação da estrutura atual a política de segurança da informação e cibernética, listar controles de prevenção e de resposta a incidentes e formalizar os incidentes e suas medidas.

7. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS EM NUVEM

Para efeito de serviços de processamento e armazenamento de dados em nuvem, fica definido com os serviços de computação em nuvem que disponíveis virtualmente de ao menos um dos serviços a seguir:

Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos que permitam implantar ou executar softwares, incluindo sistemas operacionais e aplicativos próprios e de terceiros;

Implantação ou execução de aplicativos desenvolvidos pelo Banco Arbi S.A ou por ele adquiridos, utilizando recursos computacionais de prestadores de serviços;

Execução, por meio Web (Internet), dos aplicativos implantados ou desenvolvidos por prestadores de serviços, com utilização de recursos próprios e de terceiros.

Os serviços e as alterações contratuais dos citados, **quando relevantes** acima deverão ser previamente comunicados ao Banco Central do Brasil, conforme estabelecido no Art. 15 da Resolução 4.658 de 26.04.18, no prazo mínimo de 60 (sessenta) dias antes da assinatura.

As contratações de serviços de processamento e armazenamento de dados em nuvem no Brasil e quando sediados no exterior, devem:

Estar alinhadas com as estratégias e políticas de segurança da informação e cibernética;

Possuam capacidade técnica comprovada para assegurar os serviços contratados;

Manter efetivamente a disponibilidade de acesso aos dados e informações a qualquer tempo pela instituição;

Proceder com confidencialidade, integridade, disponibilidade e recuperação dos dados e informações processadas ou armazenadas pelo prestador de serviços;
Apresentar as certificações e comprovações exigidas, quando feitas pela instituição;

Fornecer quando demandado pela instituição, os relatórios de auditoria especializada independente, por ele contratada, ou mesmo trabalhos realizados por sua auditoria interna.

Prover de informações e de recursos de gestão adequados aos serviços fornecidos para monitoramento pelo Banco Arbi S.A;

Segregar dados e identificação dos clientes do Banco Arbi S.A por meios de controles físicos ou lógicos;

Apresentar controles de acesso voltados à proteção dos dados e das informações processadas e armazenadas pelo prestador de serviços;

E possibilitar, diante autorização da instituição e sem constrangimento, o acesso a informações e aos sistemas pelo Banco Central do Brasil.

Contratar os serviços de processamento e armazenamento de dados em nuvem em países ou regiões que mantenham convênios para troca de informações, quando necessária, com o Banco Central do Brasil;

Permitir ao Banco Central do Brasil em caso de decretação de regime de resolução do Banco Arbi. S.A, obter pleno e irrestrito acesso do responsável pelo regime, aos acordos, à documentação e as informações referentes ao contrato, assim como aos dados armazenados e as informações processadas, e outras informações relacionadas aos serviços prestados;

Ficam definidas as regiões das Américas e Europa, exceto Rússia, como áreas de livre contratação pelo Banco Arbi S.A dos serviços citados nesta política;

Obrigar a notificação prévia entre as partes com prazo mínimo de 30 (trinta) dias para interrupção dos serviços por qualquer que seja o motivo.

Obrigar em caso de extinção do contrato à transferência dos dados ao novo prestador de serviços ou a algum servidor indicado pelo Banco Arbi S.A.;

Garantir a exclusão dos dados e informações transferidas, após a confirmação da integridade e da disponibilidade dos dados recebidos;

8. REPORTING ANUAL

O Banco Arbi S.A elaborará relatórios anuais, com data-base 31 de dezembro sobre:

8.1. Plano de Ação e de Resposta a Incidentes, abordando no mínimo os pontos:

A efetividade da implementação das ações;

Resumo dos resultados obtidos na implementação de rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta a incidentes, conforme diretrizes e princípios desta política;

Resumo dos incidentes relevantes relacionados com o ambiente cibernético ocorrido no período;

Resumo dos resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

8.2. Testes de Vulnerabilidades e Invasão, refletindo os resultados da análise de vulnerabilidades e testes de invasão dos Servidores Banco Arbi.

Os Relatórios anuais deverão ser apresentados à diretoria da instituição até 31 de março do ano seguinte ao da data-base.

9. DISSEMINAÇÃO DE SEGURANÇA, DIVULGAÇÃO E COMUNICAÇÃO

Em conformidade com as melhores práticas de mercado e orientação dada pela Resolução 4.658 de abril de 2018, o Banco Arbi S.A utilizará os meios descritos abaixo para difundir, esclarecer e comunicar seus colaboradores e a quem for de interesse sobre a segurança da informação e cibernética da instituição:

DISSEMINAÇÃO DA CULTURA DE SEGURANÇA DA INFORMAÇÃO E CIBERNETICA: O Banco Arbi S.A enveredará esforço para implementar programas e metodologias de capacitação e avaliação de pessoal quanto à segurança da informação e cibernética;

DIVULGAÇÃO DOS PRINCÍPIOS E DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA: O Banco Arbi S.A enveredará em toda a sua estrutura, esforços para a divulgação de suas políticas, manuais e informações com conteúdo de divulgação dos princípios, diretrizes e recomendações aos seus colaboradores e parceiros;

COMUNICAÇÃO A CLIENTES E USUÁRIOS: O Banco Arbi S.A utilizará em seus canais de comunicação, informativos sobre as precauções na utilização de seus produtos e serviços financeiros, quanto à segurança da informação e cibernética.

COMUNICAÇÃO DE OCORRÊNCIAS A ORGÃOS SUPERVISORES: Será objeto de comunicação prévia ao Banco Central do Brasil, a contratação de serviços de processamento, armazenamento de dados e de computação em nuvem e as ocorrências de incidentes relevantes em ambientes cibernéticos**.**

10. DETALHAMENTOS DE PROCEDIMENTOS

Os detalhamentos dos procedimentos estão determinados no Manual de Procedimentos de Segurança da Informação e Cibernética em conjunto com todos o arcabouço de políticas e procedimentos ligados ao Plano de Continuidade de Negócios da instituição.

11. RESPONSABILIDADES

As responsabilidades relacionadas quanto a Segurança da Informação e Cibernética encontram-se descritas abaixo:

10.1 DIRETORIA

Designar um diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes, conforme Art. 7 da Resolução 4.658 de 26.04.2018;
Aprovar a criação, revisão anual, desta política e do plano de ação e de resposta a incidentes, ou fora desse prazo em decorrência de novas exigências legais e, cancelamento da presente política.

10.2 AUDITORIA INTERNA

Realizar trabalhos/testes sobre esta política, com abrangência, profundidade adequadas, visando informar a Diretoria a necessidade de correções e implementação para melhores práticas de segurança da informação e cibernética.

10.3 TECNOLOGIA DA INFORMAÇÃO

Viabilizar de forma ampla a implantação, controle e gestão da Segurança da Informação e Cibernética do Banco Arbi S.A;
Dar suporte ao Compliance e Controles Internos para as melhores especificações de segurança conforme Diretrizes e Princípios descritos nesta política;
Relatar ao Compliance e Controles Internos os incidentes relevantes ocorridos e registrar os de menores relevância;

10.4 COLABORADORES EM GERAL

Aplicar as Diretrizes e Princípios desta política, com zelo adequado, visando proteger os bens e informações de uso da instituição contra o mal-uso e eventuais descasos com a segurança das informações por terceiros.

10.5 COMPLIANCE E CONTROLES INTERNOS

Revisar esta política e seus manuais anualmente, assim como o plano de ação e de resposta a incidentes;
Acompanhar os testes anuais do Plano de Continuidade de Negócios e seus cenários;
Relatar ao Banco Central do Brasil os incidentes relevantes ocorridos na instituição;
Emitir o Relatório Anual relativo à política de Segurança da Informação e Cibernética;
Gerenciar a implementação no Banco Arbi S.A da estrutura de Segurança da Informação e Cibernética.

10.6. DIVULGAÇÃO DA PRESENTE POLÍTICA

Para conhecimento e acesso de todos os colaboradores, esta Política é divulgada na Intranet do Banco Arbi S/A.

Elaborado: Marcelo Resende – Compliance
Revisado: Sérgio Lino – Controles Internos
Aprovado: Verônica Tavares – Diretoria