SETEMBRO 2023
VERSÃO 1

POLÍTICA DE POLÍTICA DE SEGURANÇA CIBERNÉTICA

CABCREDIT INVESTIMENTOS, FINANÇAS E PARTICIPAÇÕES LTDA
Avenida Paulista, nº 1754, Conjunto nº 7-A, 7º andar, Cerqueira César, CEP:01.310-300, São Paulo/SP

Sumário

1 OBJETIVO

A presente Política de Segurança Cibernética tem por objetivo definir princípios e diretrizes que permitam garantir a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela instituição, bem como orientar a implementação dos procedimentos e controles aqui definidos para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético em atendimento a norma em vigor.

2 ABRANGÊNCIA

Esta política aplica-se a todos os sócios, administradores, diretores e demais colaboradores da instituição, clientes, parceiros e prestadores de serviços que tenham acesso aos dados da instituição ou aos sistemas informatizados por ela utilizados.

3 PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Os princípios que regem esta política são:

- **Confidencialidade:** garantir que a informação esteja acessível somente às pessoas autorizadas;
- **Integridade:** garantir a autenticidade da informação e dos seus métodos de processamento;
- **Disponibilidade:** garantir que a informação esteja disponível às pessoas autorizadas sempre que for necessário acessá-la.

4 RESPONSABILIDADES

Devido ao porte, o perfil de risco e o modelo de negócio da instituição ficam definidas as seguintes responsabilidades:

I. Alta Administração

- Aprovar a Política de Segurança Cibernética;
- Promover a cultura de segurança cibernética na organização;
- Estabelecer recursos adequados para implementar as medidas de segurança;
- Revisar, periodicamente, a eficácia da política cibernética;
- Comunicar ao Banco Central do Brasil sobre a ocorrência de incidentes e das interrupções dos serviços relevantes que configurem uma situação de crise, bem como as providências para o reinício das atividades.

II. Gerenciamento de TI

- Executar o plano de ação e de resposta a incidentes;
- Promover a melhoria contínua dos procedimentos relacionados com a segurança cibernética;
- Realizar o registro e o controle dos efeitos de incidentes relevantes;
- Realizar periodicamente testes e varreduras para detecção de vulnerabilidades;
- Executar e manter cópias de segurança dos dados e das informações;
- Realizar a atividade de documentação referente à verificação de capacidade do potencial prestador de serviço, das práticas de governança corporativa e da avaliação da relevância do serviço a ser contratado;

- Elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes;
- Comunicar ao Banco Central do Brasil sobre a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

III. Colaboradores

- Cumprir as políticas e diretrizes estabelecidas;
- Proteger adequadamente suas credenciais de acesso;
- Relatar qualquer suspeita de atividade cibernética maliciosa;
- Participar de treinamentos de segurança cibernética.

5 DIRETRIZES DE SEGURANÇA CIBERNÉTICA

Esta política segue as seguintes diretrizes gerais:

- Atender às leis e normas que regulamentam as atividades da instituição;
- Assegurar a proteção das informações contra acessos, modificações, destruições ou divulgações não autorizadas;
- Assegurar que as informações sejam acessadas e utilizadas somente para as finalidades para as quais foram coletadas;
- Assegurar a adequada classificação dos dados e das informações relevantes para a operação da instituição;
- Estabelecer procedimentos e controles de segurança da informação para a prevenção, detecção e redução de riscos cibernéticos;
- Disseminar a cultura de segurança cibernética por meio da capacitação e avaliação dos colaboradores da instituição;
- Assegurar a aderência de terceiros relacionados aos negócios da instituição a esta política e a legislação e regulamentação aplicáveis.

5.1 Classificação dos dados e das informações

As informações sob responsabilidade da instituição serão classificadas considerando a relevância, sensibilidade, criticidade e grau de sigilo para o negócio e clientes, nos seguintes níveis:

- **Pública:** são informações que possuem caráter de domínio público e que não possuem restrições de acesso e, portanto, podem ser direcionadas ao público em geral;
- **Interna:** são informações confidenciais destinadas ao uso interno da instituição e que estão disponíveis para todos os colaboradores e partes autorizadas;
- **Restrita:** são informações altamente confidencias disponíveis apenas a colaboradores específicos da instituição, que as necessitem para exercer suas atribuições. O acesso a essas informações devem ter restrições rigorosas;
- **Confidencial:** são estão disponíveis somente para a Alta Administração e pessoas por ela autorizadas.

5.2 Cenários de incidentes

Devem ser elaborados, no âmbito dos testes de continuidade de negócios, cenários

de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela instituição, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição, levando-se em consideração para a elaboração desses cenários a ausência de ativos humanos ou tecnológicos.

5.3 Procedimentos e controles para prestadores de serviços

Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros, considerando as características do serviço a ser prestado e níveis de complexidade, abrangência e precisão, deverão ser analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

Uma vez identificados os possíveis cenários, serão analisados os controles voltados à prevenção e ao tratamento dos incidentes já utilizados pela prestadora, e, caso necessário, deverão ser estabelecidos com a respectiva prestadora de serviços outros procedimentos e controles de prevenção e tratamento dos incidentes a serem adotados, de forma a suprir as possíveis lacunas relativas à prevenção, detecção e redução da vulnerabilidade a incidentes relacionados com o ambiente cibernético.

São consideradas, para fins de aplicação do disposto nesta política, as empresas prestadoras de serviços a terceiros que tiverem acesso:

- Aos dados da instituição ou por ela controlados; ou
- Aos sistemas utilizados pela instituição; ou
- Aos ambientes físicos ou tecnológicos que possam ser utilizados para acessar os dados e sistemas da instituição.

5.4 Avaliação da relevância dos incidentes

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

6 PROCEDIMENTOS E CONTROLES

A instituição adota os seguintes procedimentos e controles para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético:

6.1 Autenticação

Para garantir a segurança dos acessos a instituição adota regras de autenticação para o sistema operacional e banco de dados, os quais utilizam dados e chaves armazenadas no banco de dados para efetuar o acesso. Sendo que o chamado de consulta do login do usuário pelo sistema é feito em ambiente criptografado por chaves

SSL.

Há sistemas que só devem ser acessados via VPN. Esses acessos deverão ser providos aos usuários pela empresa responsável pelo fornecimento do sistema ou pelo administrador de redes da CABCREDIT, caso o acesso seja realizado em servidor local. Há ainda, sistemas que exigem que a autenticação seja realizada através de um aplicativo autenticador, como o Google Authenticator, Microsoft Authenticator, dentre outros.

Acessos com a exigência de autenticação:

- Sistema de e-mail;
- Sistema de Monitoramento de Compliance;
- Consulta a base de dados (em todos os canais);
- Sistema de Armazenamento de Arquivos.

Atualmente, a instituição utiliza os seguintes serviços:

BAAS (*Bank as a Service*) – Cashway: https://cashway.io/

- **Coopcred - Sistema do Core Bancário:** Acesso via VPN. Usuário deverá informar nome de usuário e senha;
- **Sistema Gerencial CABCREDIT**: Acesso via *web browser*. Usuário deverá informar e-mail e senha;
- **Internet Banking**: Acesso via *web browser*. Usuário deverá informar o número da agência, número da conta, titularidade e senha, sendo que esta última é informada somente através de teclado virtual.

Sistema de e-mail – Task: https://www.task.com.br/

- **Webmail:** Acesso via *web browser.* Usuário deverá informar e-mail e senha;

Sistema de Monitoramento de Compliance – LGPDLITE: https://lgpdlite.com

- **LGPDLITE:** Acesso via VPN. Usuário deverá informar e-mail e senha;

Sistema de Gestão de Arquivos

- **OneDrive**: Acesso via *web browser*. Usuário deverá informar e-mail, senha e código de acesso gerado pelo App *Microsoft Authenticator;*

6.2 Criptografia

O sistema de comunicação e transmissão de dados da instituição é criptografado utilizando chave SSL em seu ambiente, as senhas e logins de acesso são criptografados.

6.3 Prevenção e detecção de intrusão

Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS e sempre que o IDS / IPS detectar ou responder a uma tentativa externa mal-intencionada, suficientemente, grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada

e procedimento de resposta é acionada.

Adicionalmente, a instituição usa um Firewall como forma de prevenção e detecção de intrusão caso utilize servidor local. Ao perceber qualquer atividade irregular, o sistema deve notificar e enviar e-mails ao Administrador da rede para que atue na resolução do problema.

6.4 Prevenção de vazamento de informações

O Banco de dados da instituição é mantido em rede interna apartado do ambiente do sistema operacional, e mantido atrás de camadas de segurança, com os softwares de monitoramento mantendo o sistema operacional seguro e estável. Ao sinal de indício de instabilidade ou tentativa de comprometer algo no sistema, é recebido um alerta, o qual é prontamente atendido na ocorrência.

Além do uso das camadas de segurança, a instituição realiza treinamentos sobre o tema para todos os colaboradores pelo menos uma vez ao ano para evitar quaisquer riscos relacionados a vazamento de informações.

6.5 Detecção de vulnerabilidades

A instituição deve manter as licenças de softwares ativas para receber todas as atualizações de segurança recomendadas e fornecidas pelos fornecedores dos sistemas. Caso a atualização não seja realizada de forma automática, caberá ao Administrador da rede da CABCREDIT garantir que os sistemas estejam atualizados na versão recomendada pelo fabricante.

6.6 Proteção contra software malicioso

Todos os sistemas e aplicativos devem ser mantidos atualizados com as últimas correções de segurança e patches disponíveis e como proteção contra códigos maliciosos mantém:

- Controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos;
- Atualização das ferramentas de proteção baseadas em assinaturas, para que estejam nas últimas atualizações disponíveis.

6.7 Mecanismos de rastreabilidade para informações sensíveis

Os sistemas contêm locais fixos onde são imputados os dados originados da instituição financeira, com base nos seus produtos e políticas.

Toda informação sensível é exclusivamente armazenada no sistema de controle de arquivos da CABCREDIT e somente pode ser acessada por usuários autenticados que possuem permissão definida pelo administrador do sistema.

6.8 Controles de acesso e de segmentação de rede

O processo de gestão dos acessos a qualquer sistema quer seja interno ou em nuvem é conduzido pela área de TI, exceções deverão ser tratadas junto a alta direção.

O acesso a qualquer sistema tecnológico é autenticado, ou seja, protegido por credenciais de acesso, certificados, tokens ou qualquer outro método seguro de identificação e autenticação.

Acessos a informações e a sistemas são permitidos apenas após dois ou mais níveis de autorização, sendo o primeiro do gestor do colaborador solicitante e o segundo do responsável pela informação ou sistema.

Os acessos de colaboradores e terceiros são desativados assim que desligados ou encerrados contratos de prestação de serviços.

As credenciais de acesso a sistemas e informações, compostas por usuário e senha, são concedidas aos Colaboradores e Terceiros para uso em atividades relacionadas a seu trabalho, pelo tempo em que perdurar seu vínculo com a instituição.

É proibido transferir, compartilhar, emprestar ou revelar a senha das credenciais de acesso concedidas pela empresa a outros colaboradores, assim como é proibido o uso de credenciais de outros colaboradores.

Todos os perfis de usuários e acessos a informações ou sistemas de média e alta criticidade são revisados periodicamente pelo respectivo responsável, seguindo os critérios de segregação da função e observando o princípio de mínimo acesso (*least privilege*) e necessidade de conhecimento (*need to know*).

6.9 Backup dos dados e das informações

Esta instituição possui um método definido para execução de cópias de segurança, o qual é executado de forma a garantir continuidade caso necessário o reestabelecimento dos dados.

Periodicamente é feita uma cópia da base de dados e armazenada em uma pasta dentro do servidor e/ou em cloud. A cópia de segurança é mantida pelo tempo necessário a atender as regras do negócio e ao definido pela legislação/normas vigentes.

6.10 Registro e controle dos efeitos de incidentes relevantes

Os incidentes são registrados com o seu devido código de prioridade conforme definido no plano de ação e resposta a incidentes, onde é descrito a forma como devem ser registrados e tratados os incidentes de segurança, sendo que nos processos e ocorrências. Caso os responsáveis verifiquem grau de importância, devem notificar responsáveis e envolvidos, e observar outros itens obrigatórios ou de interesse, além de atualizar rotinas e processos de documentos como a própria política, manuais e outros que a instituição defina como necessário.

6.11 Gestão de prestadores de serviço

Os contratos com prestadores de serviço deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, assim como cláusulas que garantam que os profissionais das empresas prestadoras de serviços a terceiros:

- Tenham conhecimento e cumpram esta política;
- Zelem e protejam o sigilo das informações da instituição;
- Cumpram as normas legais que regulamentam a propriedade intelectual e a proteção de dados e a normas vigentes relacionadas à segurança cibernética e afins do Banco Central do Brasil;
- Utilizem os dados da instituição ou os sistemas por ela utilizados, bem como os ambientes físico e tecnológico da instituição, apenas para as finalidades objeto do contrato de prestação de serviço;
- Notifiquem imediatamente qualquer violação desta Política ou outras normas.

6.12 Plano de ação e de resposta a incidentes

A presente política institui o plano de ação e de resposta a incidentes com os seguintes objetivos:

- Identificar os incidentes de segurança;
- Registrar os eventos que acarretaram problemas de segurança/continuidade;
- Direcionar medidas paliativas a incidentes ocorridos;
- Criar evidências e registros para medidas corretivas;
- Acionar o plano de continuidade dos negócios;
- Reportar os incidentes de segurança;
- Adotar iniciativas para compartilhamento de informações sobre incidentes relevantes com outras instituições.

O plano abordará detalhadamente os cenários de incidentes a serem avaliados nos testes de continuidade de negócios, considerando a avaliação de risco dos incidentes por níveis de impacto nos negócios, sendo esses níveis estipulados em Gravíssimo, Grave, Médio, Baixo e Muito Baixo.

Por meio da identificação do nível de impacto do incidente deve ser sequenciado o processo para o devido encaminhamento aos responsáveis para tratamento, conclusão e registro. A instituição definiu um relatório de Incidente de Risco Cibernético (RIRC) de forma a registrar, acompanhar e simular cenários de impacto dos incidentes de segurança.

No plano, a instituição elenca os serviços primordiais e os possíveis cenários que podem acarretar prejuízo ou parada dos negócios. Para tanto, foram mapeados cenários que apresentaram risco de interrupção a serem considerados para os testes de efetividade do plano de continuidade dos negócios, sendo estes:

- Interrupção de fornecimento de link de dados;
- Interrupção do acesso ao Banco de Dados (Sistema Operacional na nuvem).

O relatório de implementação do plano de ação anual deve ser utilizado de forma a evidenciar necessidades de revisões assim como simular e registrar os testes de

continuidade dos negócios nos cenários definidos pela administração.

Registra-se que o Plano de Ação e de Resposta a Incidentes, Plano de Continuidade dos Negócios e Relatórios de Registro, Teste e Acompanhamento complementam e integram a presente política.

6.13 Compartilhamento de Informações sobre Incidentes Relevantes

A instituição adotará iniciativas para compartilhamento de informações sobre incidentes relevantes com outras instituições de pagamentos, visando contribuir para a prevenção e redução dos riscos de segurança cibernética do sistema financeiro.

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

A instituição adotará procedimentos e práticas de governança corporativa e de gestão que serão aplicadas previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, levando-se em consideração a avaliação da relevância do serviço a ser contratado, dos riscos a que esteja exposta a instituição, bem como da capacidade do potencial prestador de serviço em realizar as atividades conforme a legislação e regulamentação aplicáveis.

7.1 Abrangência

Os procedimentos e práticas serão aplicados previamente à contratação de serviços de processamento e armazenamento de dados e de serviços de computação em nuvem.

Os serviços de computação em nuvem, prestados sob demanda e de maneira virtual, compreendem a disponibilidade de ao menos um dos serviços abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- 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.

7.2 Avaliação da relevância do serviço a ser contratado

A avaliação prévia da relevância do serviço de processamento e armazenamento de dados e de computação em nuvem a ser contratado levará em consideração:

- A criticidade do serviço;
- A sensibilidade dos dados e das informações a serem processados, armazenados

e gerenciados pelo contratado;
- A classificação dos dados e das informações quanto à relevância.

7.3 Avaliação da capacidade do potencial prestador de serviço

A instituição deve avaliar, previamente, como critérios de decisão para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, a capacidade do potencial prestador de serviço em assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da instituição aos dados e às informações a serem processadas ou armazenadas;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas;
- A sua aderência às certificações exigidas por lei e 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 usuários finais da instituição por meio de controles físicos ou lógicos;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da instituição;
- A adoção de controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos executados por meio da internet, implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviço.

7.4 Contratação de serviços prestados no exterior

De modo complementar ao item 7.3, no caso de contratação de serviços prestados no exterior, a instituição observará previamente os seguintes critérios:

- A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- Se a prestação dos serviços no exterior não causa prejuízos ao regular funcionamento da instituição e nem embaraço à atuação do Banco Central do Brasil;
- A definição dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- A previsão de alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de não existir convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser

prestados, a instituição solicitará ao Banco Central do Brasil, no prazo de 60 (sessenta) dias anteriores à contratação, autorização para a contratação do serviço.

7.5 Cláusulas contratuais

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem prever:

- 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;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
- A obrigatoriedade, em caso de extinção do contrato, de:
  a) Transferência dos dados ao novo prestador de serviços ou à instituição contratante;
  b) Exclusão dos dados pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;
- O acesso da instituição contratante a:
  a) Informações fornecidas pela empresa contratada, visando a verificar o cumprimento dessas obrigações;
  b) Informações relativas às certificações e aos relatórios de auditoria especializada;
  c) Informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição;
- 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;
- A adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil;
- A obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;
- Os contratos devem prever, ainda, cláusulas específicas para o caso de decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:
- 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 e às informações que estejam em poder da empresa contratada;

- 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) 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;
  b) A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

7.6 Comunicação da contratação ao BACEN

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

- A denominação da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- 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 referida comunicação deve ser realizada, no máximo, até 10 (dez) dias após a contratação dos serviços e as alterações contratuais que impliquem modificação dessas informações devem ser comunicadas ao Banco Central do Brasil, no máximo, até 10 (dez) dias após a alteração contratual.

8 CULTURA DE SEGURANÇA CIBERNÉTICA

A instituição adotará os seguintes mecanismos para a disseminação da cultura de segurança cibernética:

- Promover a implementação de programas de capacitação e de avaliação periódica de todos os colaboradores;
- Prestar informações aos clientes sobre precauções na utilização de produtos e serviços oferecidos;

- Comprometimento da Alta Administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

9 RELATÓRIO ANUAL

Anualmente, a instituição elaborará relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes, tendo como data-base o dia 31 (trinta e um) de dezembro de cada ano corrente.

O relatório deverá ser submetido ao Comitê de Risco, quando existente, e apresentado ao Conselho de Administração ou, na sua inexistência, à Alta Administração até 31 (trinta e um) de março do ano seguinte ao da data-base, devendo abordar:

- A efetividade da implementação das ações desenvolvidas pela instituição para adequar

suas estruturas organizacional e operacional aos princípios e às diretrizes desta política;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético, ocorridos no período;
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes de segurança.

10 DOCUMENTAÇÃO

Devem ficar à disposição do Banco Central do Brasil, pelo prazo de 05 (cinco) anos:

- O documento relativo à política de segurança cibernética;
- O documento relativo ao plano de ação e de resposta a incidentes;
- Os relatórios anuais sobre a implementação do plano de ação e de resposta a incidentes;
- A documentação sobre os procedimentos e práticas de governança corporativa e de gestão e a avaliação da capacidade do potencial prestador de serviço;
- A documentação referente à contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, prestados no exterior;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle para implementação e 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, contado o prazo referido no caput a partir da implementação dos citados mecanismos.

11 DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Para divulgação desta política a instituição adotará as seguintes ações:

- Divulgação a todos os colaboradores da instituição e às empresas prestadoras de serviços a terceiros, de forma acessível e em nível de detalhamento compatível com as funções

  desempenhadas e com a sensibilidade das informações.
- Divulgação ao público, na página da instituição na internet, do resumo contendo as linhas gerais desta política.

12 COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

Ao aprovar esta Política de Segurança Cibernética, a Alta Administração da instituição firma um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, buscando sempre se manter em conformidade com as normas e regulamentos aplicáveis, sendo guiada pelos princípios, diretrizes e práticas aqui adotadas para assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou dos sistemas de informação por ela utilizados.

13 NORMAS APLICÁVEIS

- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais);
- Lei nº 12.965/2014 (Marco Civil da Internet);

- Resolução BCB nº 85/2022;
- Normas e procedimentos internos que são periodicamente revisados e aprovados pelas alçadas competentes e com a devida publicidade.

14 VIGÊNCIA E REVISÃO

Esta política terá vigência a partir da data de aprovação pela Alta Administração, e será revisada e documentada anualmente ou a qualquer momento para se adequar a alterações regulatórias ou outras obrigações legais.