BANCO LUSO BRASILEIRO	**POLÍTICA**	**CÓDIGO: PG|15.4|10** **EDIÇÃO: novembro/2024** **Nº de PÁGINAS: 13** **VERSÃO: 5ª (interna)** **ND: 02**

PG | POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Órgão Elaborador: Segurança da Informação e Prevenção a Fraudes	**Órgão Validador: DVP/OP | Compliance**

SUMÁRIO

1. OBJETIVO

Esta Política de Segurança da Informação e Cibernética tem como objetivo estabelecer "**Princípios" e "Diretrizes"**, capazes de permitir aos colaboradores seguir padrões de comportamento desejáveis e aceitáveis, observando a legislação e as melhores práticas de mercado, com o intuito de garantir a segurança, a confidencialidade, a integridade e a disponibilidade das informações de propriedade do Banco Luso Brasileiro ("Banco") ou informações mantidas sob sua guarda e visa reforçar o comprometimento da Alta Administração com a melhoria contínua dos procedimentos relacionados à Segurança da Informação e Cibernética.

2. DOCUMENTOS COMPLEMENTARES

Código de Conduta Ética

Plano de Continuidade de Negócios v.2.2

PN|18.4|01.05: Gestão de Acesso e Utilização de Dados Corporativos

3. DOCUMENTOS DE REFERÊNCIA

Resolução CMN nº4.893|21: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Lei 13.709/2018: Lei Geral de Proteção de Dados ("LGPD")

4. DEFINIÇÕES, CONCEITOS E SIGLAS

Alta Administração: Estrutura organizacional compreendida a partir da Diretoria Estatutária e Conselho de Administração**;**

Ambiente Cibernético: Ambiente virtual no qual o usuário estabelece relações sociais;

Ameaça: Qualquer circunstância ou evento com o potencial de explorar vulnerabilidades e causar danos a sistemas, redes ou dados. Ela pode ser de natureza interna ou externa e pode incluir ações deliberadas, como ataques cibernéticos, ou acidentais, como falhas de sistemas;

ANPD: Agência Nacional de Proteção de Dados;

Ativo: Conjunto de bens e direitos do Banco;

BACEN/Banco Central do Brasil: Autarquia Federal integrante do Sistema Financeiro Nacional;

Colaboradores: Membros estatutários, funcionários, estagiários e menor aprendiz;

Criptografia: Conjunto de técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, tornando impraticável a leitura por pessoa não autorizada;

Dados Pessoais: Qualquer informação relacionada a uma pessoa física identificada ou identificável;

Diretrizes: Objetivos e ações necessárias à efetivação e manutenção do direcionamento expresso pelas políticas;

Incidente de Segurança da Informação: Todo evento que fere um ou mais princípios da Segurança da Informação (confidencialidade, integridade, disponibilidade, autenticidade e a Irretratabilidade);

Informações Corporativas: Conjunto de dados organizados que fazem sentido e que geram valor para a organização;

Instrumentos Normativos (IN): Documento que estabelece padrões classificados como Políticas, Diretrizes, Normas e Procedimentos Normativos;

Irretratabilidade: Princípio de segurança da informação por meio do qual é garantido o não repúdio às informações fornecidas;

Hardening: É o processo de reforçar a segurança de sistemas e redes, reduzindo suas vulnerabilidades por meio da remoção de funcionalidades desnecessárias, aplicação de patches, configuração segura de serviços e implementação de controles rigorosos de acesso;

Malware: Termo genérico para descrever qualquer software malicioso que visa infectar, danificar ou obter acesso não autorizado a sistemas, redes ou dispositivos. Exemplos comuns incluem vírus, worms, trojans e ransomware;

Phishing: Técnica de fraude que envolve o uso de comunicações eletrônicas enganosas, como e-mails, mensagens de texto ou sites falsificados, para enganar indivíduos e induzi-los a revelar informações confidenciais, como senhas e dados financeiros;

Política: Direcionamento expresso pela visão, missão e valores do Banco;

Princípios: Preceitos elementares ou requisitos que o Banco deve observar na realização de suas atividades, buscando uma conduta exigida nos relacionamentos, operações e serviços, em seu ambiente interno ou externo;

Proteção da Informação: Qualquer ação que tenha como objetivo preservar o valor que as informações possuem para um indivíduo ou uma organização;

Ransomware: Outro tipo de malware que “sequestra” algum dado sigiloso do usuário ou bloqueia o celular da vítima e, posteriormente, cobra pelo “resgate” dessas informações ou desbloqueio do aparelho;

Responsabilidade: Consiste na obrigação de responder corporativa ou localmente por determinadas atribuições;

Risco: Definido como a quantificação da incerteza, no contexto da segurança da informação pode ser entendido como o potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto desses ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

Risco Cibernético: Exposição a danos e perdas resultantes da ocorrência de incidentes cibernéticos;

Segurança Cibernética: Refere-se ao conjunto de práticas, tecnologias e processos utilizados para proteger redes, dispositivos, programas e dados contra-ataques cibernéticos, danos ou acessos não autorizados. Seu objetivo é garantir os cinco pilares fundamentais da segurança da informação;

Confidencialidade: Garantir que apenas as pessoas autorizadas possam acessar as informações;

Integridade: Assegurar que os dados não sejam alterados indevidamente e se mantenham precisos e confiáveis;

Disponibilidade: Garantir que as informações e sistemas estejam acessíveis quando necessários;

Autenticidade: Verificar a identidade das partes envolvidas no acesso e na manipulação de informações;

Irretratabilidade (não-repúdio): Assegurar que ações ou transações não possam ser negadas pelas partes envolvidas;

Terceiros: Parceiros de negócio, prestadores de serviços e fornecedores;

Vulnerabilidade: Fragilidade ou falha em um sistema, software ou processo que pode ser explorada por uma ameaça para causar danos ou obter acesso não autorizado. As vulnerabilidades podem resultar de falhas de design, implementação ou configuração inadequada;

Vírus: Tipo de *malware* que infecta outros arquivos, alterando seu conteúdo, de forma que eles passem a ter códigos maliciosos;

Worm: Ao invés de infectar outros arquivos, este tipo de malware procura se espalhar para outros dispositivos, como por exemplo através de e-mail e mensagens via app de mensagens.

5. ABRANGÊNCIA

Estão obrigados a observar, cumprir e fazer cumprir os termos e condições desta política e demais regulamentos correlatos, os **colaboradores** do Banco em qualquer nível hierárquico, na sua esfera de competência, zelando pela materialização, realização eficaz das regras e princípios da segurança e proteção da informação, no compromisso com os critérios legais e éticos que envolvem o banco, aplicando-se as mesmas orientações para terceiros.

6. DETALHAMENTO

6.1. Princípios

6.1.1. Princípios | Gerais

Ética e Legalidade: Atuar em conformidade com a legislação e regulação vigentes, com padrões de ética e conduta.

Transparência: Garantir a lisura do negócio para fortalecer os laços entre as partes interessadas, garantindo que haja boas relações e engajamento.

Melhoria Contínua: Compromisso de aperfeiçoar os padrões de ética e conduta, aplicação de medidas corretivas, adequados níveis de segurança, qualidade dos produtos ofertados, eficiência dos serviços.

6.1.2. Princípios | Segurança da informação

Confidencialidade: Garantir que o acesso às informações seja restrito apenas às pessoas autorizadas, prevenindo o uso indevido de dados sensíveis;

Integridade: Assegurar que as informações não sejam alteradas indevidamente, mantendo sua exatidão e confiabilidade, de modo a evitar a modificação não autorizada de dados;

Disponibilidade: Garantir que as informações e sistemas estejam acessíveis e operacionais sempre que necessário, permitindo que os processos de negócio funcionem sem interrupções;

Autenticidade: Verificar a identidade das partes envolvidas no processo de acesso e manipulação das informações, assegurando que os dados e sistemas sejam acessados apenas por usuários devidamente autenticados;

Irretratabilidade (Não-repúdio): Assegurar que nenhuma das partes envolvidas em uma transação ou comunicação possa negar a autoria de suas ações ou transações realizadas, garantindo rastreabilidade e responsabilidade.

6.2. Diretrizes

A fim de proteger as informações, o Banco estabelece diretrizes a serem seguidas, visando a implementação de controles de segurança que permeiam seu compromisso e responsabilidade com a segurança da informação por todos os níveis hierárquicos, sendo tais diretrizes as seguintes:

1. As informações do Banco, clientes e usuários, colaboradores e terceiros devem ser tratadas de forma ética, sigilosa e legal, evitando-se mau uso e exposição indevida;
2. Classificar os dados e as informações quanto a sua relevância;
3. O controle e o tratamento da informação de acesso restrito ficam limitados às pessoas que tenham necessidade de conhecê-la;
4. Definir parâmetros a serem utilizados para identificar a relevância dos eventos;
5. Utilizar mecanismos de segurança (Banco e terceiros) atualizados e modernos que acompanham a evolução tecnológica do mercado capazes de prestar suporte e proteção correspondentes ao Banco;
6. Utilizar as informações de forma transparente e apenas com a finalidade para a qual foi coletada;
7. Garantir identificação única a cada colaborador sendo pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
8. Assegurar que senhas de acesso sejam mantidas secretas e atribuídas a cada colaborador, sendo realizado aculturamento quanto a proibição de seu compartilhamento;
9. Elaborar cenários de incidentes a serem considerados nos planos de contingência de negócios;
10. Definir procedimentos e controles preventivos e de tratamento dos incidentes a serem adotados por empresas terceiras que manuseiam dados ou informações sensíveis, ou relevantes para as atividades operacionais;
11. Implementar ações de capacitação e avaliação periódica;
12. Manter ações informativas aos clientes e usuários quanto as precauções na utilização de produtos e serviços financeiros;
13. Reportar para a área de Segurança da Informação todos os riscos relacionados às informações do Banco e seus clientes, para que sejam analisados, avaliados e tratados de acordo com a situação.

6.3. Governança

O Banco desde a sua concepção, preza pela relevância dos ativos de informação no mercado financeiro, de modo que as informações produzidas ou recebidas devem ser utilizadas com senso de responsabilidade, de modo ético e seguro em benefício exclusivo dos negócios corporativos.

Desse modo, para exercer de forma aprimorada a atividade bancária, o banco se baseia em princípios primordiais de segurança da informação, a fim de preservar, monitorar e tratar a propriedade da informação de maneira eficiente, observando sua confidencialidade, integridade e disponibilidade.

A área de Segurança da Informação deve orientar os processos de levantamento, avaliação e tratamento das vulnerabilidades e das ameaças capazes de deixar os ativos de informação em situação de risco considerada inaceitável pelo Banco Central do Brasil.

Assim, devem ser implementados controles e procedimentos específicos, incluindo aqueles voltados à rastreabilidade da informação, visando prevenir, detectar e reduzir vulnerabilidades técnicas, processuais e jurídicas, minimizando os riscos de incidentes relacionados ao Ambiente Cibernético, de forma a garantir a segurança das informações.

6.4. Abrangência do Conteúdo

O conteúdo desta política deve ser compatível com o porte, o perfil de risco e o modelo de negócio do Banco, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos do Banco, a sensibilidade dos dados e das informações sob sua responsabilidade, observando os princípios e diretrizes definidos pela alta administração para implementação de procedimentos que visem assegurar a confidencialidade, a integridade e a disponibilidade das informações detidas e utilizadas pelo Banco.

6.5. Regras e Procedimentos

6.5.1. Tratamento das Informações

As informações corporativas devem ser classificadas de acordo com seu grau de importância, sigilo e disponibilidade em dados relevantes, dados sensíveis e classificadas por níveis que tratam informações confidenciais, uso interno e pública e deve abranger os serviços de processamento, armazenamento de dados e de computação em nuvens prestados no país ou no exterior, devendo estas serem disponibilizadas somente a pessoas autorizadas, visando a redução/mitigação de riscos como vazamentos e compartilhamentos indevidos.

6.5.2. Medidas de controle

O Banco deve monitorar e registrar o uso das informações tratadas e veiculadas em seu ambiente, estabelecendo procedimentos e controles, como trilhas de auditoria e registros de atividades em todos os pontos e sistemas que entender necessário, para reduzir a vulnerabilidade a incidentes de segurança de dados, bem como outras adversidades que possam vir a ocorrer, destaca-se as seguintes medidas técnicas a serem adotadas como: autenticação; prevenção a vazamento de informações; testes de intrusão; varredura de vulnerabilidades; controle contra software malicioso; Criptografia, rastreabilidade; segmentação de rede; manutenção de cópias de segurança dos dados e das informações.

O Banco deverá realizar uma análise robusta dos resultados de atividade de monitoramento, bem como definir a periodicidade de revisão do nível de sensibilidade das informações, quando necessário.

6.5.3. Contratação de Terceiros

O processo de contratação de terceiros relevantes que tratam informações dentro ou fora das dependências do Banco, devem ser orientados por regras e procedimentos claros a serem observados com rigor e devem se comprometer e agir de acordo com essa Política, observando e respeitando os pilares da Segurança da Informação, tais quais: Confidencialidade, Integridade e Disponibilidade.

No caso de qualquer nova contratação, alteração, adequação ou encerramento de contratos vigentes que se enquadrem nesta Política, deverá ser informada às áreas de Segurança da

Informação e Prevenção a Fraudes e Jurídico para providências internas de efetivação ou do encerramento do relacionamento.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, deve ser comunicada ao Banco Central do Brasil, contendo a denominação da empresa contratada, os serviços relevantes contratados e 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, bem como alterações contratuais ocorridas nessas informações, sendo observado o prazo de dez dias após a contratação ou alteração dos serviços.

6.5.4. Ações de Aculturamento e Responsabilidades

Os colaboradores, parceiros, prestadores de serviços e fornecedores relevantes do Banco, devem ter conhecimento dessa Política, versão interna e/ou externa conforme o caso, sendo comunicada e divulgada adequadamente.

Os colaboradores e terceiros relevantes que realizem qualquer forma de acesso, manipulação de informações ou utilização de recursos tecnológicos do Banco devem se comprometer e agir de acordo com essa Política, observando e respeitando os pilares da Segurança da Informação.

6.5.5. Treinamento e Capacitação

O Banco promoverá periodicamente, treinamentos para os seus colaboradores e terceiros relevantes sobre a presente Política, no início de relacionamento ou quando de atualizações, e, aplicar testes de avaliação da assimilação do conteúdo para os conhecimentos adquiridos.

6.5.6. Gestão e Monitoramento da Segurança da Informação

O Banco deve monitorar e registrar o uso das informações tratadas e veiculadas em seu ambiente de modo a viabilizar o monitoramento, por meio de controles apropriados, trilhas de auditoria e registros de atividades em todos os pontos e sistemas que entender necessário, a fim de reduzir os riscos de incidentes e visando a manutenção das boas práticas.

6.5.7. Continuidade de Negócios

Os planos de continuidade de negócios devem assegurar o tratamento dos incidentes relevantes e situações de contingência relacionados com o ambiente cibernético, definindo os procedimentos a serem seguidos no caso da 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 o reestabelecimento da operação normal do Banco, bem como os cenários de incidentes considerados nos testes de continuidade de negócios.

6.5.8. Plano de Ação e de Resposta a Incidentes de Segurança Cibernética

O Banco deve possuir documento específico contendo o plano de resposta a incidentes de segurança, para orientar a Gestão de Crise de Incidente, com ações a serem desenvolvidas pelo banco para adequar sua estrutura organizacional e operacional aos princípios e às diretrizes da Política de Segurança da Informação e Cibernética;

6.5.9. Relatório anual

O Banco deverá elaborar relatório anual, com data-base de 31 de dezembro, sobre a implementação do plano de ação e de resposta a incidentes destacando a efetividade das ações, resultados obtidos, os incidentes relevantes e os testes de continuidade de negócios. O presente relatório, deve ser submetido ao comitê de gestão de riscos e aprovação da alta administração.

6.6. Responsabilidades

6.6.1. Conselho de Administração

1. Aprovar a Política de Segurança da Informação e Cibernética e o plano de ação e de resposta a incidentes;
2. Obter ciência sobre o relatório anual de implementação do plano de ação e de resposta a incidentes até 31 de março do ano seguinte ao da data-base.

6.6.2. Gestores

1. Garantir em suas respectivas áreas a implementação de mecanismos necessários para o descarte seguro das informações;
2. Demonstrar zelo e conhecimento sobre Segurança da Informação, mostrando-se como referência de conduta para os colaboradores internos sob a sua gestão;
3. Assegurar que suas equipes possuam acesso e conheçam esta política, bem como os procedimentos aqui estabelecidos;
4. Especificar e solicitar previamente permissão de acesso, elencando os ativos de informação para prestadores de serviços em geral;
5. Nos casos de contratação de Terceiros e Prestadores de Serviços, sempre utilizar o *template* de contrato ou semelhante contendo as cláusulas de segurança da informação e cibernética, devidamente avaliada pelo Jurídico;
6. Analisar de forma crítica os incidentes identificados, compartilhando com a área de Segurança da Informação e Prevenção a Fraudes para a definição conjunta das ações necessárias;

6.6.3. Colaboradores

1. Utilizar adequadamente as ferramentas e equipamentos de trabalho disponibilizados;
2. Utilizar a internet, a ferramenta de e-mail e outros dispositivos e equipamentos do Banco, com foco somente nas atribuições profissionais de maneira responsável;
3. São responsáveis pela segurança das informações a que tiverem acesso, inclusive quando em regime não presencial;
4. Manter equipamentos corporativos como notebooks e celulares bloqueados quando da não utilização, devendo permanecer guardados em local seguro quando não estiverem sendo utilizados, sendo considerada falta grave quando da ausência do devido cuidado;
5. Buscar orientação do superior hierárquico, quando houver dúvidas relacionadas à segurança da informação;
6. Assinar o Termo de Responsabilidade, formalizando a ciência da Política de Segurança da Informação e Cibernética, bem como assumindo a responsabilidade pelo seu cumprimento;
7. Comunicar a área de Segurança da Informação e Prevenção a Fraudes sobre qualquer descumprimento ou violação desta política e procedimentos relacionados a ela;
8. São responsáveis pela manutenção do sigilo de suas senhas de acesso aos recursos, sistemas e serviços da rede de computadores, sendo vedada a utilização da conta de identificação dos usuários por terceiros;

9. Não abrir mensagens de remetentes desconhecidos, pois pode se tratar de um ataque *Phishing*. Sempre que identificada uma mensagem suspeita, informar a equipe de Segurança da Informação e Prevenção a Fraudes através do e-mail si@lusobank.com.br. Nunca devem ser abertos arquivos, links ou anexos de remetentes desconhecidos.

6.6.4. Segurança da Informação e Prevenção a Fraudes

1. Assegurar a devida segregação de função nos sistemas do Banco, mitigando o risco de conflito de acessos;
2. Revisar anualmente os acessos dos sistemas, a fim de realizar adequações em usuários/perfis/sistemas necessários;
3. Participar da implantação de novos sistemas do Banco, a fim de definir ou direcionar os perfis de acesso dos usuários, assegurando a devida segregação de função já na implantação;
4. Coordenar o Comitê de Segurança da Informação e Privacidade dos Dados;
5. Apresentar anualmente as melhorias e respostas à incidentes através de Relatório anual regulamentar;
6. Revisar anualmente o Plano de Continuidade de Negócios, realizando a atualização, se necessário, dos documentos relacionados;
7. Registrar eventuais ocorrências relevantes ocorridas, as principais ações tomadas para solução e planos de ação quando necessário, para mitigação de riscos identificados;
8. Comunicar e promover treinamentos periódicos de colaboradores e parceiros em relação à Segurança da Informação e Continuidade de Negócios;
9. Promover a gestão da Segurança da Informação no que se refere aos processos corporativos;
10. Revisar, quando se fizer necessário, a Política de Segurança da Informação e Cibernética e, após a aprovação do Conselho de Administração, acompanhar sua publicação nos canais disponíveis para conhecimento dos envolvidos;
11. Estar em conformidade com a legislação pertinente e vigente.

6.6.5. Segurança da Informação e Prevenção a Fraudes | Tecnologia da Informação

1. Promover a gestão da segurança da informação no que se refere aos processos tecnológicos e ferramentas utilizadas;
2. Analisar tecnicamente os incidentes de Segurança Cibernética;
3. Atuar na implementação de soluções para melhoria contínua da Segurança Tecnológica;
4. Promover o processo de *Hardening* do ambiente tecnológico;
5. Monitorar o ambiente tecnológico, realizando a atualização e análise de tentativas de ataques identificadas;
6. Atuar em situações que necessitem de investigação Forense, quando necessário; comunicar imediatamente à Diretoria e ao Encarregado (“DPO”) sobre incidentes que tenham como consequência o vazamento de Dados Pessoais sobre tratamento do Banco, independente de quem sejam os titulares dos dados vazados;
7. Fornece ao DPO as informações e demais subsídios a respeito dos incidentes, a fim de viabilizar o atendimento e/ou reporte de informações a que o Banco está obrigado, seja para a ANPD, BACEN e/ou titulares dos Dados Pessoais.

6.6.6. Comitê de Segurança da Informação e Privacidade de Dados

O Comitê de Segurança da Informação e Privacidade de Dados – CSIPD, formado por representantes das áreas de Segurança da Informação e Prevenção Fraudes, Jurídica, Desenvolvimento Organizacional (RH), Compliance / Marketing, Controles Internos, Produtos, Auditoria e Tecnologia da Informação (TI), possuem as seguintes responsabilidades:

1. Definir estratégias que promovam e reforcem a Segurança da Informação e Privacidade dos Dados do Banco;
2. Avaliar ações para a conscientização de todos os colaboradores, terceiros e prestadores de serviços quanto à relevância da Segurança da Informação e Privacidade dos Dados para o negócio do Banco;
3. Identificar pontos de melhorias de Segurança da Informação e Privacidade dos Dados dentre os processos do Banco;
4. Formalizar a análise de causa e impacto, bem como controles relacionados aos efeitos de incidentes relevantes;
5. Definir medidas a serem tomadas para os casos de descumprimento da Política de Segurança da Informação e Cibernética;
6. Emitir relatório técnico de segurança cibernética, fornecendo informações sobre eventuais incidentes de segurança cibernética e eventuais melhorias/fragilidades nos sistemas do Banco;
7. Avaliar quando demandado, o relatório anual sobre a implementação do plano de ação e de resposta a incidentes e enviar para aprovação do Diretor de Segurança Cibernética;
8. Revisar, anualmente, os procedimentos de Gestão de Crise de Incidente de Segurança, o qual aborda especificamente as Diretrizes do plano de ação e resposta a incidentes;

6.6.7. Diretor Responsável pela Política de Segurança da Informação e Cibernética

O Diretor responsável pela Política, também deverá colocar em execução o plano de ação e de resposta a incidentes, quando necessário, assim como exercer as seguintes funções:

1. Comunicar a Diretoria e o Conselho de Administração sobre os riscos relevantes de segurança cibernética e eventuais incidentes ocorridos, bem como as medidas adotadas no plano de ação e de resposta a incidentes;
2. Orientar o Comitê de Segurança da Informação e Privacidade de Dados em situações de dúvidas quanto à Política e plano de ação de resposta a incidentes;
3. Revisar e aprovar o relatório anual sobre a implementação do plano de ação e de resposta a incidentes.

6.6.8. Jurídico

1. Apoiar o Comitê de Segurança da Informação e Privacidade de Dados nas questões específicas a sua área que se relacionem com Segurança da Informação e Cibernética no momento da contratação de serviços relevantes, conforme prevê o art. 13, da Resolução 4.893/21, bem como no tocante às comunicações ao BACEN;
2. Adequar os contratos e apontar os riscos nas contratações utilizando como base a Lei Geral de Proteção de Dados Pessoais (LGPD);
3. Responsável em analisar os contratos e distratos realizados com fornecedores de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

6.6.9. Formalização

1. Responsável por arquivar contratos e distratos realizados com os fornecedores de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem para disponibilizar ao BACEN, caso solicitado.

6.6.10. Auditoria Interna

1. Avaliar a adequação e a conformidade dos processos e procedimentos relacionadas à política, auditando e testando os mecanismos para acompanhamento, controle e mitigação de riscos e a sua eficácia e efetividade, de acordo com planejamento anual.

6.6.11. Encarregado ("DPO")

1. Apoiar as áreas de Tecnologia e Segurança da Informação e Prevenção a Fraudes em assuntos e demandas relacionadas à legislação que dispõe sobre o tratamento de dados pessoais, emitindo pareceres, bem como fornecendo subsídios para tomada de decisão pela diretoria.
2. Realizar a interlocução entre o Banco e a Agência Nacional de Proteção de Dados ("ANPD") em assuntos relacionados ao tratamento de dados pessoais pelo Banco.

6.7. Penalidades

Todos os colaboradores do Banco, incluindo parceiros comerciais, fornecedores e prestadores de serviços, conforme mencionando na versão "externa" da Política de Segurança da Informação e Cibernéticas, que deixem por negligência, culpa ou dolo, de cumprir as obrigações previstas nas políticas internas, e na lei, estão sujeitos a ações disciplinares, incluindo a rescisão do contrato e/ou medidas administrativas ou criminais, além das penalidades previstas em lei.

As infrações à Política de Segurança da Informação e Cibernética e suas regras deverão ser informadas à área de Segurança da Informação e Prevenção a Fraudes, por meio do e-mail: si@lusobank.com.br, que promoverá a apuração através de procedimentos internos.

Qualquer caso de não cumprimento da Política da Segurança da Informação e Cibernética, por uma área, cliente, parceiro comercial, fornecedores e prestadores de serviços, devem ser comunicados seguindo o procedimento interno, com o adequado detalhamento da razão do não cumprimento | violação, além dos controles compensatórios existentes ou definidos e os riscos residuais.

7. VIGÊNCIA

Esta Política entra em vigor na data de sua publicação e vigorará por prazo indeterminado, devendo ser revisada, no mínimo, anualmente ou, quando necessário, caso haja alguma mudança nas normas internas do Banco, na alteração de Diretrizes de Segurança da Informação e Cibernética, nos objetivos de negócio e, ainda, caso seja requerido pelo órgão regulador competente.

8. HISTÓRICO DAS REVISÕES

Versão	Aprovador	Data de Revisão	Descrição
2ª	DVP/OP	04/04/2022	Revisão e atualização da área

3ª	DVP/OP	16/08/2022	Revisão e atualização da área
4ª	DVP/OP	Setembro 2023	Revisão e atualização da área
5ª	DVP/OP	novembro 2024	Revisão e atualização da área

9. ANEXOS

Sequencial	Título

10. APROVAÇÃO

Órgão Aprovador | Diretoria	
Membro	**Assinatura**
José Francisco Fernandes Ribeiro	
João Miguel Loureiro Martins	
Ernani Leite Vitorello	

Órgão Aprovador | Conselho de Administração	
Membro	**Assinatura**
Marta Cláudia Ramos Amorim Barroca de Oliveira	
Jorge Manuel Seabra de Freitas	

Paulo José Dinis Ruas	
Maurício Lourenço da Cunha	