BANCO LUSO BRASILEIRO o banco que fala a sua língua	**POLÍTICA**	**CÓDIGO: PG|15.4|10.1** **EDIÇÃO: Agosto/2021** **Nº de PÁGINAS: 10** **VERSÃO: 1ª** **ND: 3**

PG | POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA EXTERNA

Órgão Elaborador: CI | Segurança	**Órgão Validador: DVP/OP | Compliance**

SUMÁRIO

1. OBJETIVO

Esta política de Segurança da Informação e Cibernética **"Política"** tem como objetivo estabelecer "**Princípios" e "Diretrizes"**, capazes de permitir aos nossos colaboradores seguir padrões de comportamento desejáveis e aceitáveis, de acordo com a legalidade e boas práticas, com o intuito de garantir 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

3. DOCUMENTOS DE REFERÊNCIA

Resolução CMN nº 4.893|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.

Resolução CMN nº 4.658|18: 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 financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

4. DEFINIÇÕES, CONCEITOS E SIGLAS

Alta Administração: Estrutura organizacional compreendida a partir da Diretoria Estatutária e Conselho de Administração da Instituição Financeira**.**

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

Ativo: Algo que tenha valor para o Banco.

BACEN| Banco Central do Brasil: Autarquia Federal integrante do Sistema Financeiro Nacional.

Colaboradores: Membros estatutários, funcionários, estagiários e menor aprendiz da Instituição Financeira.

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: Evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação.

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.

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.

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

Riscos: Evento hipotético, cuja ocorrência pode afetar de forma positiva ou negativa uma organização.

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

Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos ao Banco.

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 à informação seja obtido somente por pessoas autorizadas e quando for, de fato, necessário;

Integridade: Garantir a exatidão e completude da informação e dos métodos de seu processamento, bem como da transparência no tratamento com as pessoas envolvidas;

Disponibilidade: Garantir que as pessoas autorizadas tenham acesso à informação, sempre que necessário e devidamente autorizado.

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 relevância;
3. Definir parâmetros a serem utilizados para identificar a relevância dos eventos;

4. Utilizar mecanismos de segurança (Banco e terceiros) atualizados e modernos que acompanham a evolução tecnológica do mercado capazes de prestar suporte e proteção correspondentes a uma instituição financeira;
5. Utilizar as informações de forma transparente e apenas para a finalidade para a qual foi coletada;
6. Garantir identificação única a cada colaborador sendo pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
7. Assegurar que senhas de acesso sejam mantidas secretas e atribuídas a cada colaborador, sendo realizado aculturamento quanto a proibição de seu compartilhamento;
8. Elaborar cenários de incidentes a serem considerados nos planos de contingência de negócios;
9. Definir procedimentos e controles preventivos e de tratamento dos incidentes a serem adotados por empresas terceiras que manuseiem dados ou informações sensíveis, ou relevantes para as atividades operacionais;
10. Implementar ações de capacitação e avaliação periódica;
11. Manter ações informativas aos clientes e usuários quanto a precauções na utilização de produtos e serviços financeiros;
12. 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.

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

6.4. Serviços de computação em nuvem

Para interpretação dessa Política, conforme previsto no art. 13 da Resolução 4.893/2021, considera ao menos um dos seguintes serviços de computação em nuvem que abrangem a disponibilidade do Banco Luso Brasil, sob demanda e de maneira virtual:

1. 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;
2. Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;

3. Execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

6.5. Divulgação e Declaração de Responsabilidade

Todos os colaboradores, parceiros, prestadores de serviços e fornecedores relevantes do Banco possuem conhecimento dessa Política pelos seguintes meios:

1. Via ações internas de Segurança da Informação;
2. Por meio digital, através da *intranet* corporativa;
3. Por meio digital em formato reduzido, através do site institucional.

Os colaboradores, parceiros, prestadores de serviço e fornecedores 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.

O Banco promove, periodicamente, treinamentos para os seus colaboradores, parceiros, prestadores de serviço e fornecedores relevantes sobre a presente Política, no início de relacionamento ou quando de atualizações, e, aplica testes de avaliação da assimilação do conteúdo para os conhecimentos adquiridos.

6.6. Classificação das Informações

As Informações Corporativas foram classificadas de acordo com seu grau de importância, sigilo e disponibilidade.

6.6.1. Informações relevantes ou sensíveis

1. Dados cadastrais de clientes e colaboradores;
2. Financeiras e de carteira de clientes e colaboradores;
3. Contratos;
4. Contábeis da Instituição;
5. Regulatórias;
6. Jurídicas;
7. De Recursos Humanos;
8. Tecnológicas;
9. Fornecedores que processam e | ou armazenam dados;
10. Fornecedores que processam e | ou armazenam dados em nuvem.

O Banco deverá ter cautela ao tratar Informações corporativas classificadas como relevantes ou sensíveis, devendo estas serem disponibilizadas somente a pessoas autorizadas, visando a redução | mitigação de riscos como vazamentos e compartilhamentos indevidos.

6.6.2. Níveis de classificação

1. **Confidencial:** São informações de acesso restrito a um colaborador ou a um específico grupo de colaboradores, sendo que sua divulgação pode violar a privacidade, bem como acordos de confidencialidade.
2. **Uso Interno**: São informações disponíveis aos colaboradores para orientação a execução de suas atividades não sendo destinada ao público externo.

3. **Pública**: São informações aprovadas pelo responsável direto para consulta irrestrita sendo que a divulgação externa não compromete o negócio não precisando de procedimentos de proteção efetiva ou tratamento específico.

6.7. Contratação de Terceiros

Todos os Parceiros, Prestadores de serviço e Fornecedores Relevantes que tratam informações dentro ou fora das dependências do Banco, além de observarem os instrumentos normativos relacionados à Contratação de Terceiros, deverão cumprir e fazer cumprir as seguintes determinações:

1. Certificar total conhecimento dos requisitos a serem cumpridos nos contratos firmados, alinhados a legislação e regulamentação vigente;
2. Fornecer acesso ao Banco aos dados e às informações a serem processados ou armazenados no momento da prestação de serviços;
3. Quando solicitado, responder ao questionário de adoção de práticas de governança corporativa e de gestão;
4. Observar os princípios basilares da Segurança da Informação, tais quais: confidencialidade, a integridade, a disponibilidade, bem como a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
5. Comprovar a aderência às certificações exigidas pela instituição para a prestação do serviço a ser contratado, quando solicitado;
6. Autorizar o acesso do Banco 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;
7. Disponibilizar informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
8. Identificar e proceder com a segregação dos dados dos usuários finais do Banco por meio de controles físicos ou lógicos;
9. Garantir qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais do Banco;
10. No caso da execução de aplicativos por meio da *internet,* deve-se adotar controles que mitigam os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo;
11. Certificar total conhecimento sobre todos os itens desta política e firmar termo de responsabilidade, assumindo o compromisso para o cumprimento integral de todos os itens nela constantes.

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, Controles Internos e Jurídico para providência internas de efetivação do encerramento do relacionamento.

O Banco ao efetuar a contratação de determinado parceiro, prestador de serviços e fornecedor, com o qual serão compartilhados informações confidenciais e sensíveis, observa o que se segue:

1. Assegurar que a contratação não poderá causar prejuízos ao regular funcionamento do Banco, tampouco qualquer embaraço à atuação do Banco Central do Brasil;

2. Definir, em momento anterior à contratação, quais os países e as regiões em cada país onde os serviços poderão ser prestados e os dados e informações poderão ser armazenados e processados;
3. Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato;
4. Analisar a criticidade do serviço e o nível da sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados, considerando a classificação dos dados e das informações quanto à relevância;
5. Documentar a avaliação de capacidade técnica do fornecedor e parceiro.

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.

6.8. Medidas de prevenção para clientes e usuários

O Banco trabalha diariamente para manter seu ambiente cibernético seguro, tornando a segurança da informação a sua prioridade, o que é visível em suas políticas e procedimentos.

Em contrapartida, é essencial destacar que a responsabilidade pela segurança da informação também depende de seus clientes e usuários, os quais devem estar atentos às “pegadinhas”, “golpes cibernéticos” e softwares maliciosos que circulam pela internet.

Os cibercriminosos, por meio dos artifícios supracitados, buscam a obtenção de dados e informações de forma ilícita, para, assim, angariar vantagens indevidas.

Dessa forma, a fim de orientar os clientes e/ou usuários a colaborarem para a manutenção de um ambiente online seguro, o Banco Luso Brasileiro recomenda o que se segue.

6.9. Autenticação

A responsabilidade pelo uso dos meios de autenticação/identificação, como *logins* e senhas, pertencem ao cliente/usuário que mantém a posse de tais dados sigilosos. Nesse sentido, o Banco recomenda:

1. Os dados de identificação (*login* e senha) devem ser memorizados, não sendo registrados em outros ambientes digitais ou físicos, tampouco informados a terceiros, ainda que sejam de seu convívio familiar. Tal medida corrobora para a manutenção da confidencialidade de suas informações;
2. A senha deve ser alterada não apenas periodicamente, mas sempre que suspeitar da violação de sua confidencialidade;
3. Deve ser elaborado senhas de qualidade, o que significa dizer que devem ser fortes - contendo letras, números, caracteres especiais) e únicas, não devendo ser repetidas;
4. Não deve ser autorizado o uso do equipamento pessoal do cliente e/ou usuário por outras pessoas enquanto estiver conectado com sua identificação;
5. O equipamento pessoal do cliente e/ou usuário deve estar sempre bloqueado em caso em que ele for se ausentar do local;

6. Deve ser habilitado o método de autenticação por dois fatos. Por exemplo: E-mail, Token, SMS, etc.).

6.10. Antivírus

Atualmente, o cliente e/ou usuário deve se preocupar com a ativação do antivírus diariamente. As suas definições devem sempre estar atualizadas e instaladas no computador ou dispositivo utilizado para acesso aos serviços digitais do Banco.

Importante ressaltar que a utilização de antivírus desatualizado, ou com a proteção em tempo real desativada, impacta completamente em sua eficiência, deixando os dispositivos mais vulneráveis a ataques cibernéticos dos mais diversos, bem como a softwares maliciosos.

6.11. Phishing

A técnica denominada Phishing é caracterizada por tentativas de adquirir informações e dados pessoais de diversos tipos, como senhas, dados financeiros (número de cartões de crédito e conta bancária), bem como outros dados.

Nesse tipo de ataque cibernético, o fraudador se faz passar por uma pessoa ou empresa confiável, enviando uma comunicação oficial por meio de e-mail, mensagem instantânea, SMS, contato telefônico, entre outros.

Exemplo

1. O fraudador procura atrair as atenções dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade;
2. O fraudador tenta se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de Comércio Eletrônico, *Market Place*, entre outros sites populares;
3. O fraudador tenta induzir os usuários a preencher formulários com os seus dados pessoais e/ou financeiros ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos internautas.

Dessa forma, o Banco recomenda que os clientes e/ou usuários sempre se certifiquem da origem do e-mail, SMS, contato telefônico, contatando diretamente o Banco, se o caso.

6.12. Malwares | *Softwares* Maliciosos

Os *Malwares* se referem a *softwares i*ndesejados que visam causar danos aos dispositivos, realizando alterações e até mesmo o roubo de informações.

Tais softwares ganham forma infectando o dispositivo através de vírus, *worms*, trojans e *spywares*, que chegam até o usuário através da técnica de *Phishing* ou a instalação de software que o usuário julga ser confiável.

A fim de evitar que o dispositivo seja infectado por tais softwares, O Banco recomenda as iniciativas que se seguem:

1. O antivírus deve estar sempre atualizado, bem como a funcionalidade de executar varreduras diárias deve estar habilitada;
2. O usuário deve estar sempre em alerta quanto aos e-mails recebidos, especialmente aqueles que tentam convencê-lo a realizar determinadas ações suspeitas;
3. Deve-se evitar sites suspeitos.

6.13. Spam

O termo *Spam* é utilizado normalmente para e-mails indesejados enviados para muitas pessoas, possuindo conteúdo com fins publicitários.

Cabe destacar que mensagens publicitárias indesejadas em sites também são consideradas *Spam*, estando diretamente associadas a ataques cibernéticos, uma vez que são responsáveis também pela propagação de *Malwares*, venda ilegal de produtos e disseminação de golpes.

Assim, algumas medidas devem ser consideradas a fim de evitar a proliferação deste tipo de ameaça ao seu dispositivo, quais sejam:

1. O usuário deve evitar responder uma mensagem de *Spam* que tenha origem desconhecida - nem mesmo para se descadastrar -, pois tal ação possibilita que o autor do *Spam* confirme que aquele e-mail é ativo, enviando novos *Spams* para a vítima;
2. O usuário não deve encaminhar mensagens de *Spam*;
3. O usuário não deve distribuir endereços de e-mail, devendo utilizar a funcionalidade: “cópia oculta”.

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.