Denominação			
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA			
Área Emitente	**Número**	**Emissão**	**Atualização**
Segurança da Informação| Controles Internos	**P02.01_VP**	**Fev/2019**	**Fev/2019**

I. Objetivos da Segurança da Informação e Cibernética

a) Ressaltar o comprometimento da Alta Administração com a melhoria contínua dos procedimentos relacionados à Segurança da Informação e Cibernética.

b) Estabelecer diretrizes que permitam aos colaboradores do Banco Luso Brasileiro seguir padrões de comportamento desejáveis e aceitáveis de acordo com a legalidade e boas práticas, a fim de mitigar riscos técnicos e jurídicos;

c) Implantar controles específicos que permitam a rastreabilidade da informação para garantir a Segurança das Informações "sensíveis".

d) Definir procedimentos específicos para reduzir a vulnerabilidade a incidentes cibernéticos, buscando preservar a segurança das informações sob a guarda e domínio do Banco.

e) Preservar as informações do Banco Luso Brasileiro quanto à confidencialidade, integridade e disponibilidade, seja de colaboradores, clientes, fornecedores e terceiros

f) Minimizar os riscos de perdas financeiras, de participação no mercado, de imagem, da confiança de clientes e parceiros ou de qualquer outro impacto ao negativo no negócio do Banco Luso Brasileiro resultante de uma falha de segurança.

II. Diretrizes da Política de Segurança da Informação e Cibernética

O Banco Luso Brasileiro estabelece os controles e diretrizes para a proteção das informações. Esses controles são denominados diretrizes e são apresentados a seguir:

a) As informações do Banco Luso Brasileiro, de seus clientes e parceiros devem ser tratadas de forma ética, sigilosa e legal, evitando-se mau uso e exposição indevida;

b) As informações devem ser utilizadas de forma transparente e apenas para a finalidade para a qual foi coletada;

c) As senhas de acesso devem ser mantidas secretas, sendo proibido seu compartilhamento;

d) Todos os riscos relacionados às informações do Banco Luso Brasileiro e seus clientes devem ser reportados para a área de Segurança da Informação| Controles Internos e Tecnologia, para que sejam analisados, avaliados e tratados de acordo com a situação.

III. Abrangência

Todas as regras aqui estabelecidas devem ser aplicadas a todos os colaboradores, fornecedores e parceiros relevantes no que se refere à proteção da informação.

IV. Princípios da Política de Segurança da Informação e Cibernética

As informações do Banco Luso Brasileiro, produzidas ou recebidas deverão ser utilizadas com senso de responsabilidade e de modo ético e seguro, em benefício exclusivo dos negócios corporativos baseado nos seguintes princípios:

a) Confidencialidade: Garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando for, de fato, necessário;

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

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

V. Divulgação e Declaração de Responsabilidade

A Política de Segurança da Informação e Cibernética deve ser de conhecimento de todos os colaboradores, prestadores de serviços e parceiros relevantes.

Todos os colaboradores, fornecedores e parceiros relevantes, além de prestadores de serviços que realizem qualquer forma de acesso, manipulação de informações ou utilizem recursos tecnológicos do Banco Luso Brasileiro, devem se comprometer e agir de acordo com a Política de Segurança da Informação e Cibernética, respeitando os pilares básicos da Segurança da Informação: Confiabilidade, Intergridade, Disponibilidade.

VI. Classificação das informações

As informações corporativas foram enquadradas considerando o seu grau de importância, sigilo e disponibilidade. São consideradas como relevantes as que estão relacionadas a:

a) Dados cadastrais de clientes e colaboradores;
b) Financeiras e de carteira de clientes e colaboradores;
c) De contratos;
d) Contábeis da Instituição;
e) Regulatórias;
f) Jurídicas;
g) De Recursos Humanos;
h) Tecnológicas;
i) De Fornecedores que processam e/ou armazenam dados;
j) De Fornecedores que processam e/ou armazenam dados em nuvem.

Informações corporativas classificadas como relevantes (sensíveis), devem ser tratadas com cautela e disponíbilizadas somente a pessoas autorizadas, com o intuito de mitigar possíveis riscos de vazamentos e de compartilhamentos indevidos.

VII. Contratação de Fornecedores e Parceiros Relevantes

Todos os fornecedores e parceiros que processam e/ou armazenam informações relevantes conforme critérios estabelecidos nesta política, deverão cumprir as seguintes definições:

a) Ciência de todas as cláusulas da Resolução 4658/2018 do Banco Central do Brasil, em particular o art. 17, firmando o compromisso para o pleno cumprimento de todos os itens nela estabelecida;

b) Ciência de todos os itens desta política;

c) Assinar o termo de responsabilidade, firmando o compromisso para o cumprimento integral de todos os itens desta política.

Controle de Elaboração e Aprovação

Elaboração	Validação / Revisão	Aprovação
Gestor Segurança da Informação	**Diretoria**	**Conselho de Administração**

Diretoria,

_____
José Francisco Fernandes Ribeiro

_____
João Miguel L. Martins

_____
Willy Otto Jordan

Conselho de Administração,

Marta Claudia R. A. B. Oliveira	**Paulo Jose Dinis Ruas**
Maurício Lourenço Da Cunha	**Jorge Manuel Seabra de Freitas**