Política de Segurança Cibernética

Versão 1.0.

Controlo de Elaboração

	Nome do Responsável	Função	Rubrica	Data
Elaboração	Soraya Lopes	DORG		30-07-2020
Verificação	Cristiana Lavrador	Administração		30-07-2020
Aprovação	Natalino Lavrador	PCA		30-07-2020

Nota: O Documento original encontra-se assinado pelo Conselho de Administração e arquivado sob a responsabilidade do Conselho de Administração.

Mapa de Revisões

Número de Versão	Data	Motivo	Observações
1.0.	22-09-2020	Elaboração inicial	

Alterações desde a Última Versão

Alterações	n/a

Documento

Sumário	
Documentos a revogar	n/a
Documentos Complementares	Política Global de Segurança de Informação; Manual de Normas de Segurança do Sistema de Informação.

Índice

1 INTRODUÇÃO

A presente política pretende demonstrar, em alinhamento com os valores do BCH, as medidas que tem implementadas para proteger os dados e informação de clientes, colaboradores e parceiros, nomeadamente dados pessoais e financeiros.

Esta política foi elaborada nos termos das disposições do Aviso nº08/2020, de 02 de Abril, do Banco Nacional de Angola.

2 APLICAÇÃO

A Política de Segurança Cibernética é aplicada a todos os membros dos órgãos sociais, a todos os colaboradores, parceiros e partes interessadas que, por sua vez, venham a ter contacto com qualquer activo de informação do Banco, nomeadamente dados, sistemas, equipamentos e infra-estruturas.

As directrizes de segurança cibernética são igualmente aplicáveis a todos os sistemas, dados e informações do Banco independentemente do seu formato, estado (armazenada, em transito ou em processamento) ou fase do ciclo de vida.

Entende-se por:

a) Colaborador: todos os colaboradores, estagiários e mandatários, a título permanente ou ocasional, independentemente da natureza do seu vínculo com o Banco;

b) Parceiro: entidade (colectiva ou singular) com quem o Banco tem uma relação profissional e contratual, para fim de atingir objectivos específicos;

c) Parte interessada: todos os elementos (pessoas, instituições, grupos, órgãos governamentais, etc.) que de alguma forma afectam ou são afectados pela organização.

Qualquer questão relacionada com o conteúdo da política ou respectiva aplicação, deverá ser endereçada à Direcção de Sistemas de Informação (DSI) do Banco.

Qualquer incumprimento da mesma será avaliado pela DSI e, em caso específicos pela o Jurídica, Auditoria Interna e de Compliance, para determinar as acções a tomar.

3 SEGURANÇA CIBERNÉTICA

O Banco implementa diversas iniciativas com o objectivo de promover um ambiente de segurança cibernética que salvaguarde, de forma adequada, dos dados e informação geridos pelo Banco. Estas iniciativas são alinhadas e suportadas por reconhecidos regulamentos e referências de mercado referentes à segurança cibernética.

Apresentam-se as medidas aplicadas pelo Banco de modo a garantir a protecção dos seus dados, informação, sistemas e infra-estruturas:

a) Alinhamento das suas políticas, processos e procedimentos internos com as melhores práticas do mercado, nomeadamente:

   i. ISO/IEC 27000 – Família de normativos para a gestão da segurança da informação;

   ii. ISO 31000 – Família de normativos para a gestão do risco;

   iii. NIST *Cybersecurity Framework* – *Framework* para a segurança computacional.

b) Aplicação dos requisitos regulamentares referentes à segurança cibernética, nomeadamente:

   i. Aviso N° 08/2020 do Banco Nacional de Angola – Regulamento referente à gestão da Política de Segurança Cibernética e Adopção de Computação em Nuvem;

   ii. SWIFT CSP – Programa anual de segurança da informação, que discrimina os requisitos de controlo a serem implementados no sistema de gestão de mensagens interbancárias (SWIFT);

   iii. PCI DSS – Normativo com requisitos de segurança a ser aplicados a dados de cartões de pagamento.

c) Desenvolvimento de políticas e normativos internos que estabelecem os requisitos a ser implementados por forma a garantir a protecção dos dados e informação geridas pelo Banco. Encontram-se endereçados os seguintes domínios:

   i. Gestão do risco da segurança da informação;

ii. Gestão de incidentes de segurança cibernética;

iii. Gestão de identidades e acessos aos dados, sistemas e infra-estruturas;

iv. Gestão de vulnerabilidades técnicas;

v. Segurança de informação em serviços na nuvem;

vi. Regras e requisitos de criptografia;

vii. Utilização aceitável dos sistemas de informação.

d) Promoção e desenvolvimento de sessões de formação aos seus colaboradores sobre temas relacionados com a segurança cibernética;

e) Contratualização de serviços externos e independentes de auditorias de risco aos sistemas de informação e sistema de controlo interno do Banco;

f) Execução de testes e auditorias técnicas de segurança periódicas aos seus sistemas de informação.

4 RESPONSABILIDADES

O Banco, com o apoio da sua administração, tem a responsabilidade de:

a) Implementar as medidas técnicas e organizacionais para mitigar riscos de segurança cibernética;

b) Garantir que se encontram implementadas as salvaguardas necessárias para proteger a informação dos seus clientes, colaboradores e parceiros;

c) Avaliar e monitorizar continuamente os riscos de segurança cibernética a que o Banco se encontra exposto;

d) Garantir a melhoria contínua do seu ambiente de segurança cibernética;

e) Garantir a protecção dos interesses vitais dos seus clientes, colaboradores e parceiros;

f) Manter-se actualizado relativamente a tendências de segurança cibernética;

g) Formar e sensibilizar os seus colaboradores para os riscos e boas práticas de utilização dos activos de informação do Banco;

h) Aplicar as medidas necessárias para investigar e responsabilizar não conformidades com as directrizes definidas.

5 DOCUMENTOS COMPLEMENTARES

A aplicação da presente Política deverá ser complementada com os demais códigos, políticas, ou normativos internos relacionados com os domínios em questão, nomeadamente:

a) Política Global de Segurança de Informação;

b) Manual de Normas de Segurança do Sistema de Informação;

c) Outros normativos internos em vigor.

6 REVISÃO E COMUNICAÇÃO

A Política de Segurança Cibernética será objecto de revisão sempre que se verifiquem alterações internas e/ou externas com impactos importantes sobre a mesma. O acompanhamento da sua aplicação será assegurado pela Direcção de Sistemas de Informação, que reportará à Administração do BCH as eventuais ocorrências.

A presente Política será divulgada no site do Banco www.bch.co.ao, e estará também acessível na rede interna do Banco a todos os colaboradores.