YETU

Tradição e Inovação

Política de Segurança Cibernética

ÍNDICE

1| INTRODUÇÃO

1.1| SUMÁRIO

Os activos de informação assumem um papel crítico no desenvolvimento e sustentabilidade da estratégia e negócio do Banco YETU, SA (Banco), por este motivo é essencial que estes activos sejam protegidos e salvaguardados de forma que não sejam ultrapassados os limiares de risco aceites pelo Banco. O Banco YETU reconhece que um incidente de Segurança da Informação pode causar uma interrupção nas suas operações de negócio, comprometer a sua reputação e, inclusive, ter consequências legais, regulamentares e financeiras.

1.2| OBJECTIVOS

A Política de Segurança Cibernética do Banco YETU visa garantir a protecção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pelo Banco para o alcance dos objetivos de segurança da informação.

A Política de Segurança Cibernética demonstra o compromisso do Banco YETU em zelar e tratar as informações dos seus Clientes, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Demonstrando o compromisso com os aspectos regulatórios e estratégicos do Banco, estando assim, em conformidade com as principais regulamentações vigentes.

1.3| ÂMBITO

No cumprimento dos normativos legais, regulamentares e das recomendações da entidade reguladora sobre a necessidade de estabelecerem-se regras sobre a componente da Segurança Cibernética, o Banco YETU implementou um conjunto de controlos, dos quais políticas, processos, procedimentos, estruturas organizacionais e tecnologias, de forma a assegurar a confidencialidade, integridade e a disponibilidade das redes, dados e dos sistemas de informação.

Todos os Clientes do Banco YETU e Partes Interessadas devem ter acesso e conhecimento formal da política de Segurança Cibernética.

É da responsabilidade da Direcção de Organização e Qualidade (DOQ) garantir a publicação e divulgação da Política Segurança da Informação.

1.4| ENQUADRAMENTO LEGAL E REGULAMENTAR

A Política de Segurança Cibernética do Banco está alinhada com as disposições legais e regulamentares, nomeadamente:

- Lei N.º 40/20 – Lei do Sistema de Pagamentos de Angola
- Lei N.º 14/21 - Lei do Regime Geral das Instituições Financeiras
- Lei N.º 22/2011 – Lei da Protecção de Dados Pessoais
- Aviso N.º 08/2020 – Política de Segurança Cibernética e Adopção de Computação em Nuvem
- Aviso N.º 12/2016 – Protecção dos Consumidores de Produtos e Serviços Financeiros
- Directiva 05/DSB/DRO/2022
- ISO/IEC 27001
- ISO/IEC 27005
- ISO/IEC 31000

2| CONCEITOS

Para efeitos desta política, entende-se por:

Activo de Informação: Activo (físico ou Digital) que armazena, processa ou transfere informação do Banco.

Acesso: Privilégios que um Utilizador/Conta tem para aceder a dados, sistemas, serviços ou infraestruturas do Banco;

Confidencialidade: Propriedade que a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados;

Disponibilidade: Propriedade da informação ser acessível e utilizável a pedido de uma entidade autorizada;

Integridade: Garantia da consistência, completitude e exactidão da informação e respectivos métodos de processamento, durante todo o seu ciclo de vida;

Risco de Segurança da Informação: Risco de ser comprometida a confidencialidade, integridade ou disponibilidade de um activo de informação;

Responsável do Risco: pessoa ou entidade com a responsabilidade e autoridade para gerir um risco;

Cibersegurança: é um conjunto de ações e técnicas criadas destinadas a protecção de sistemas, programas, redes e equipamentos contra intrusões.

Incidente de Cibersegurança: Evento ou um conjunto de eventos que comprometem ou podem comprometer a informação e/ou os sistemas de informação, incluindo actos ou omissões, deliberados ou não que violem as políticas de Segurança de Informação do Banco.

Incidente de Cibersegurança Significactivo: Incidente que resulta no incumprimento com obrigações legais ou regulamentares.

Incidente de Cibersegurança Muito Significactivo: Incidente com potencial risco sistémico para o sistema financeiro Angolano.

Prestadores de serviços: Entidade externa que fornece qualquer tipo de serviços para o apoio à actividade do Banco.

Evento de Cibersegurança: Ocorrência que pode ter um significado de segurança, i.e. pode representar uma ameaça à confidencialidade, integridade e disponibilidade de um activo tecnológico.

Vulnerabilidade: Falha técnica num sistema de informação que pode ser potencialmente explorada com o intuito de serem executadas acções não autorizadas no sistema de informação.

Vulnerabilidade Zero Day: Vulnerabilidades até à data desconhecidas para quais não existe uma medida de mitigação conhecida.

3| RESPONSABILIDADES

3.1| COMISSÃO EXECUTIVA

1. Definir e aprovar o plano, estratégia e objectivos de Segurança da Informação;
2. Assegurar os recursos necessários para a gestão e operacionalização da Política de Segurança Cibernética;
3. Patrocinar as principais iniciativas que contribuam para que as metas de Segurança da Informação do Banco sejam atingidas.
4. Monitorizar a execução do plano de Segurança da Informação;
5. Identificar e propor os recursos (pessoas, tecnologias, infraestruturas, financeiros, etc.) necessários à execução do plano de Segurança da Informação.
6. Garantir a realização das revisões, avaliações e testes da segurança da informação para a identificação eficaz de vulnerabilidades dos sistemas e serviços.

3.2| GABINETE DE SEGURANÇA

1. Identificar, promover e gerir a implementação de controlos, iniciativas e projectos de Segurança da Informação;
2. Desenvolver e melhorar as políticas e normativos internos de Segurança da Informação;
3. Garantir a correcta identificação, gestão e monitorização dos riscos de segurança da informação do Banco;
4. Formar e sensibilizar os Colaboradores do Banco para os temas de Segurança da Informação;
5. Promover a cultura de Segurança de Informação no Banco;
6. Incentivar o cumprimento das directrizes de Segurança da Informação, junto das equipas técnicas e áreas de negócio do Banco;
7. Estabelecer uma comunicação regular com a gestão de topo do Banco, por forma a comunicar e definir planos de tratamento para riscos identificados.

3.3| DIRECÇÃO DE TECNOLOGIAS E SISTEMAS DE INFORMAÇÃO

1. Garantir a implementação de controlos, iniciativas e projectos tecnológicos de Segurança da Informação, previstos no Plano de Segurança da Informação;
2. Acompanhar e monitorizar as actividades de operação de segurança;
3. Garantir a operacionalização de actividades relacionadas com a gestão de incidentes de segurança da informação;
4. Apoiar o Gabinete de Segurança na promoção a cultura de Segurança de Informação no Banco;
5. Apoiar na identificação, avaliação e implementação de tecnologias que suportem os objectivos de segurança do Banco.

3.4| DIRECÇÃO DE DESENVOLVIMENTO DE PESSOAS

1. Apoiar o Gabinete de Segurança na dinamização de iniciativas de formação e consciencialização dos Colaboradores do Banco, relativamente a Segurança da Informação;
2. Garantir a aplicação dos requisitos de Segurança da Informação relactivos à gestão do ciclo de vida da relação contratual de Colaboradores com o Banco;
3. Reportar à Direcção de Tecnologias e Sistemas de Informação quaisquer alterações relevantes de relação contratual com os Colaboradores bem como participar do processo de revisão de acessos.

3.5| CLIENTES

1. Garantir a responsabilidade quanto a confidencialidade, integridade e disponibilidade da informação a que têm acesso;
2. Garantir a correcta utilização durante o uso dos serviços digitais os activos do Banco.

4| INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais, colectadas e armazenadas pelo Banco YETU é restrito aos profissionais autorizados ao uso dessas informações sempre que necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas ou fins, devendo respeitar, ainda, o disposto na política de Classificação da Informação.

O Banco YETU poderá em certos momentos ter de fazer a partilha de dados pessoais com terceiros de acordo a legislação vigente no país.

Entidades que podem vir a solicitar dados pessoais:

1. Administração Geral Tributária;
2. Banco Nacional de Angola;
3. BODIVA;
4. Comissão de Mercados de Capitais;
5. Correspondentes Bancários;
6. Procuradoria-Geral da República;
7. Tribunais;
8. Unidade de Informação Financeira.

5| ESTRUTURA DA GESTÃO DA SEGURANÇA CIBÉRNETICA

A gestão dos controlos da Segurança Cibernética assegura que os procedimentos operacionais sejam desenvolvidos, implementados ou modificados de acordo com os objetivos estabelecidos nesta Política.

5.1| GESTÃO DE ACESSOS ÀS INFORMAÇÕES

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente, e cancelados tempestivamente ao término do contrato de trabalho do Colaborador ou do prestador de serviço.

Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controlo de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os Colaboradores do Banco YETU devem ter sessões de treinamento periodicamente no que diz respeito aos riscos cibernéticos e as medidas de controlo da segurança da informação, através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética.

5.2| PROTECÇÃO DO AMBIENTE DO BANCO

São constituídos controlos e responsabilidades pela gestão e operação dos recursos de processamento das informações, com o objectivo de garantir a segurança na infraestrutura tecnológica do Banco YETU por intermédio de um modelo de gestão efetivo no que diz respeito ao monitoramento, tratamento na resposta aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura da infraestrutura de comunicações e sistemas.

5.2.1. AUTENTICAÇÃO

Os acessos às informações e aos ambientes tecnológicos do Banco YETU é permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

O controlo de acesso aos sistemas é formalizado e contempla, no mínimo, os seguintes controlos:

1. A utilização de identificadores (credencial de acesso) individualizados, monitorados e passíveis de bloqueios e restrições (automatizados e manuais);
2. A remoção de autorizações dadas a Colaboradores afastados ou desligados do Banco YETU, ou ainda que tenham mudado de função;
3. A revisão periódica das autorizações concedidas.

5.2.2| GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O comportamento de possíveis ataques é identificado por meio de controles de detecção implementados no ambiente, como Filtro de aplicações, ferramenta de detecção de comportamentos maliciosos, Antivírus, Anti-spam, Anti-malwares, entre outros.

5.2.3| PREVENÇÃO A FUGA DE INFORMAÇÕES

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou divulgados nas redes sociais ou outros canais digitais por Colaboradores não autorizados.

5.2.4| TESTES DE INTRUSÃO

Testes de intrusão interno e externo nos canais digitais do Banco (*SiteYETU, NetYETU*), devem ser realizados anualmente.

5.2.5| VERIFICAÇÕES DE VULNERABILIDADES

As verificações na infraestrutura interna e externa devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

5.2.6| CONTROLO CONTRA SOFTWARE MALICIOSO

Todos os activos (computadores, servidores, etc.) que estejam conectados à rede corporativa ou façam uso de informações do Banco YETU, são compatíveis, e protegidos com uma solução *anti-malware* determinada pela área de Segurança da Informação.

5.2.7| CRIPTOGRAFIA

Toda solução de criptografia utilizada no Banco YETU está parametrizada com as regras e os padrões de segurança da Informação.

5.2.8| MONITORIZAÇÃO

Todos os sistemas do Banco YETU enviam os seus ficheiros de *Logs* para uma plataforma de gestão e correlação de eventos com o intuito de fazer o devido controlo de todo o tráfego gerado na sua infraestrutura de comunicação e sistemas. Exemplo de *Logs*:

1. Autenticação de Colaboradores (tentativas válidas e inválidas);
2. Acesso a informações;
3. Acções executadas pelos Colaboradores, incluindo criação ou remoção de dados no sistema.

5.2.9| SOLUÇÕES DE SOFTWARE SEGURAS

O Banco YETU mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projectada e implementada no ciclo de vida de desenvolvimento de sistemas.

52.10| COPIAS DE SEGURANÇA (BACKUP)

O processo de execução de *backups* é realizado, periodicamente, nos activos de informação do Banco YETU, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

5.3| CONTINUIDADE DE NEGÓCIO

O processo de continuidade de negócios do Banco YETU esta desenhado com o intuito de reduzir os impactos e perdas de activos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

Incluem-se nesse processo, a continuidade de negócios relactivos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

6| PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA PARA OS CLIENTES

6.1| AUTENTICAÇÃO E SENHA

O Cliente é responsável pelos actos executados com seu identificador (*login* / sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.
Recomendamos que:

1. Mantenha a confidencialidade, memorize e não registe a senha em qualquer lugar. Ou seja, não contar a ninguém e não anotar em papel;
2. Alterar a senha sempre que existir qualquer suspeita que alguém possa ter visto a mesma;
3. Elaborar senhas de qualidade, de modo que sejam complexas e difíceis de serem descobertas;
4. Impedir o uso do seu equipamento (telemóvel, computador) por outras pessoas, enquanto este estiver a utilizar os serviços digitais do Banco com a sua identificação;
5. Bloquear sempre o equipamento ao ausentar-se.
6. Sempre que possível, habilitar um segundo factor de autenticação (Por exemplo: SMS, Token e etc.).

6.2| ANTIVÍRUS

Recomendamos que o Cliente mantenha uma solução de antivírus actualizada e instalada no computador ou outro equipamento que utilize para ter acesso aos serviços oferecidos pelo Banco. De preferência ter sempre estes dispositivos actualizados com as versões de OS mais recentes.

6.3| ENGENHARIA SOCIAL

A engenharia social, no contexto de segurança da informação, refere-se à técnica pela qual uma pessoa procura persuadir a outra, muitas vezes abusando da ingenuidade ou confiança do utilizador, com objectivo de ludibriar a mesma, aplicando golpes a fim de obter informações sigilosas.

6.3.1| PHISHING

Técnica utilizada por ciber-criminosos para enganar os utilizadores, através de envio de *e-mail's* maliciosos, a fim de obter informações pessoais como senhas, cartão de crédito, número de identificação pessoal, número de contas bancárias, entre outros. As abordagens dos *e-mail's* de *phishing* podem ocorrer das seguintes maneiras:

1. Procuram atrair as atenções das pessoas, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade, ou quer seja por caridade;
2. Tentam passar-se pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de Comércio Eletrónico, entre outros sites populares;
3. Tentam induzir as pessoas a preencher formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de *softwares* maliciosos que possuem o objectivo de recolher informações sensíveis;

6.3.2| SPAM

São *e-mails* não solicitados, os quais geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os *spams* estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

6.3.3| FALSO CONTACTO TELEFÓNICO

São técnicas utilizadas por pessoas criminosas para conseguir informações como dados pessoais, senhas, *token*, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

7| CONFORMIDADE LEGAL

7.1| CONFORMIDADE COM OBRIGAÇÕES LEGAIS, REGULAMENTARES E CONTRATUAIS

1. O Banco precisa manter um registo com as obrigações legais, regulamentares e contratuais em matéria de Segurança da Informação e protecção de dados pessoais.
2. É preciso ser mapeada, por cada obrigação legal, regulamentar e contratual em matéria de Segurança da Informação e protecção de dados pessoais a área do Banco YETU responsável por assegurar a sua conformidade.
3. Sempre que aplicável, a Política de Segurança da Informação do Banco YETU, bem como os processos operacionais de Segurança da Informação, devem ser ajustados para assegurar o cumprimento com novas obrigações legais, regulamentares e contratuais do Banco YETU em matéria de Segurança da Informação.

7.2| DIREITOS DE PROPRIEDADE INTELECTUAL E LICENCIAMENTO

1. O Banco YETU possui procedimentos de uso de *Software* licenciados, respeitando desta forma os direitos de propriedade intelectual do *software* instalado nos sistemas de informação para suporte às actividades de negócio do Banco.

2. Não é permitido a reprodução/cópia de *software* licenciado no Banco, ou a instalação deste tipo de *software*, sem que seja validado e autorização pela Comissão Executiva.

7.3| RETENÇÃO DE DADOS

1. O Banco tem a necessidade de manter um registo com os prazos de retenção de dados afim de cumprir obrigações legais, regulamentares, contratuais e de negócio.
2. Para evitar que exista um excesso de informação não útil para o Banco, é preciso a implementação de mecanismos de expurgo de dados para assegurar que os dados são eliminados, de forma segura, sempre que forem atingidos os prazos máximos definidos, quer os dados estejam residentes em suporte físico (ex. papel) ou suporte digital (ex. bases de dados, ficheiros, *backups*).