Política de Resiliência Cibernética

(Cyber Resilience Policy)

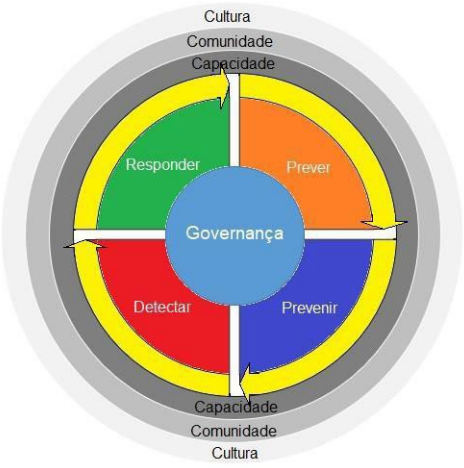
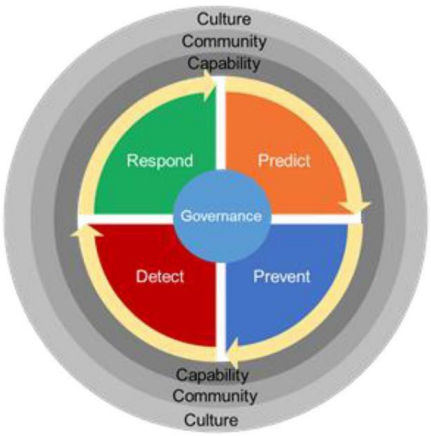
Nome do Documento: *Document Name:*	Política de Resiliência Cibernética. *Cyber Resilience Policy*
Nível: *Level:*	Standard Bank de Angola, S.A. *Standard Bank de Angola, S.A.*
Tipo: *Type:*	Política *Policy*
Responsável: *Standard Owner:*	Director de Segurança da Informação *Head of Information Security (CISO)*
Aprovado por: *Approved by:*	Comité de Tecnologias e Segurança da informação, Dados e Operações do Conselho de Administração *Board Technologies and Information Security, Data and Operations*
Data de Aprovação: *Approval Date:*	(Modificada)24 de Março de 2026 *(Modified) March 24, 2026*
Data de Revisão: *Review Date:*	(Modificada)24 de Março de 2027 *(Modified) March 24, 2027*

	Versão em português / Portuguese version	*English version / Versão em inglês*
1	**Introdução**	**Introduction**
1.1	O Standard Bank Angola (SBA) adota princípios sólidos de governança corporativa, um dos quais é o uso e aplicação de políticas e normas que definem e articulam princípios dentro dos quais o Grupo Standard Bank (SBG) opera. O SBA usa os guias do SBG para definir e articular as normas mínimas de tecnologia, práticas de suporte, bem como as ferramentas, técnicas e processos. Todas as normas de tecnologia são sustentadas pelos valores, código de ética, estratégia de tecnologia e o exercício de bom senso de indivíduos responsáveis.	he Standard Bank Angola subscribes to sound corporate governance principles, one of which is the use and application of policies and standards which define and articulate principles within which the SBG Group will operate. SBA uses technology playbooks to define and articulate minimum SBG standards, supporting practices, tools and techniques. All technology standards are underpinned by the group values, code of ethics, the group technology strategy and the exercise of good judgement by responsible individuals.
2	**Aplicabilidade**	**Applicability**
2.1	De acordo com o modelo integrado operacional da organização, as normas de tecnologia são adoptadas e executadas nos países membros do Grupo, unidades de negócios e funções corporativas. Se houver um requisito do SBG que não está refletido na regulamentação local, o país irá cumprir com os requisitos locais. De igual forma, os países devem garantir que cumprem com requisitos regulatórios locais específicos. Caso as actividades de segurança de tecnologias de informação sejam terceirizadas ou coordenadas por terceiros, os termos desta norma serão aplicados.	In keeping with the integrated operating company archetype, group technology standards are taken and executed by legal entities, business lines and corporate functions. If there is an SBG requirement that is not reflected in local regulation, the country will comply with local requirements. Equally, if there are specific local regulatory requirements with which entities must comply, they must ensure they do so. If technology security activities have been outsourced or are conducted by third parties, the terms of this standard shall be applied.
3	**Requisitos Mínimos Para Cumprir esta Política**	**Minimum Requirements to Comply with this Policy**
	Para garantir que esta norma seja implementada, executada e cumprida as seguintes responsabilidades foram alocadas:	To ensure that this standard is implemented, executed and complied with the following responsibilities have been allocated:
3.1	O Comité de Tecnologias e Segurança da informação, Dados e Operações do Conselho de Administração aprova a norma com base na recomendação do Comité de Gestão de Risco, e	The Board Technologies and Information Security, Data and Operations approves the standard based on the recommendation of Risk Management Committee, and includes it in the register of

	inclui a mesma no registo de Políticas de Segurança da Informação, nomeia o Responsável pela Norma e confirma uma supervisão de governança adequada;	Information Security Standards, appoints the Responsible for the Standard and confirms adequate governance oversight;
3.2	O Director de Segurança da Informação é o proprietário desta norma que poderá delegar a responsabilidade de implementação da mesma ao Gestores das áreas de Segurança da Informação;	The Head of Information Security (CISO) is the owner of this standard who may delegate the responsibility for its implementation to the Managers of the Information Security areas;
3.3	Os Gestor das áreas de Segurança da Informação são os responsáveis pela custódia e avaliam qualquer não conformidade material ou conformidade parcial da norma;	The Information Security Managers are responsible for custody and assess any material non-compliance or partial compliance with the standard;
3.4	Os órgãos governança de Segurança da Informação supervisionam a aderência as normas de tecnologia do SBA. Utilizando uma abordagem de aplicação ou explicação (a aplicação de normas é assumida e uma explicação é fornecida para todas as excepções);	Information Security governance bodies oversee adherence to SBA technology standards. Using an application or explanatory approach (the application of standards is assumed, and an explanation is provided for all exceptions);
3.5	O Director de Segurança da Informação garante que a revisão desta norma seja feita sempre que necessário.	The Head of Information Security (CISO) ensures that this standard is reviewed whenever necessary.
4	**Princípios Gerais**	**General principles**
4.1	**A Dimensão, Perfil de Risco e o Modelo de Negócios**	**The Size, Risk Profile and Business Model**
4.1.1	O SBA é reconhecido como uma instituição financeira de grande dimensão e relevância sistémica no mercado angolano, cujo modelo de negócio está orientado para os segmentos Corporativo e de Investimentos, Pequenas e Médias Empresas, e Particulares e Privada. A instituição promove produtos e serviços financeiros adaptados às necessidades específicas de cada segmento, assegurando a conformidade com as normas prudenciais, regulatórias e de segurança em vigor. O Banco adopta uma postura prudente e conservadora relativamente aos riscos operacionais, tecnológicos e de cibersegurança, com a	SBA is recognized as a large financial institution with systemic relevance in the Angolan market, whose business model is oriented towards the Corporate and Investments, Small and Medium Enterprises, and Individuals and Private segments. The institution promotes financial products and services tailored to the specific needs of each segment, ensuring compliance with the prudential, regulatory and security standards in force. The Bank adopts a prudent and conservative stance regarding operational, technological and cybersecurity risks, with the implementation of control, monitoring and continuous mitigation mechanisms that ensure the resilience,

	implementação de mecanismos de controlo, monitorização e mitigação contínua que asseguram a resiliência, confidencialidade, integridade e disponibilidade da informação.	confidentiality, integrity and availability of information.
4.2	**A Natureza da Operações, Complexidade dos Produtos, Serviços, Actividades e Processos**	**The Nature of Operations, Complexity of Products, Services, Activities and Processes**
4.2.1	O SBA disponibiliza um portefólio diversificado de produtos e serviços financeiros, caracterizado por um nível de complexidade reduzida e ajustada às necessidades dos seus segmentos de mercado. As suas operações abrangem diferentes áreas, incluindo concessão de crédito, captação de depósitos, realização de transferências, gestão de protocolos e outros serviços complementares, todos suportados por processos e procedimentos operacionais devidamente formalizados e controlados.	SBA offers a diversified portfolio of financial products and services, characterized by a low level of complexity and adjusted to the needs of its market segments. Its operations cover different areas, including granting credit, taking deposits, making transfers, managing protocols and other complementary services, all supported by duly formalized and controlled operational processes and procedures.
4.3	**Sensibilidade dos Dados e das Informações Corporativas e de Negócios**	**Sensitivity of Corporate and Business Data and Information**
4.3.1	O SBA assegura que todos os dados e informações sob a sua custódia são tratados, armazenados e processados de forma segura, com base nos princípios de confidencialidade, integridade, disponibilidade e rastreabilidade da informação. O tratamento da informação observa as melhores práticas internacionais de segurança da informação e protecção de dados, bem como o cumprimento rigoroso das normas e regulamentações aplicáveis.	SBA ensures that all data and information in its custody are treated, stored and processed securely, based on the principles of confidentiality, integrity, availability and traceability of information. The processing of information observes the best international practices in information security and data protection, as well as strict compliance with applicable rules and regulations.
5	**Princípios Padrão**	**Standard Principles**
	A Direcção de Segurança da Informação do Banco é responsável pelo desenvolvimento, implementação e manutenção do programa de resiliência cibernética. O programa está alinhado à estratégia de tecnologia do SBG, matrix de ameaça, apetite ao risco e a framework de segurança tecnológica, garantindo a conformidade com a legislação e os regulamentos relevantes. A framework é necessária para controlar	The Bank's Information Security Unit is responsible for developing, implementing, and maintaining the cyber resilience program. The program is aligned with SBG's technology strategy, threat matrix, risk appetite and technological security framework, ensuring compliance with relevant legislation and regulations. The framework is necessary to control how the Bank protects its technological assets,

	como o Banco protege seus activos tecnologicos, que incluem sistemas em produção, sistemas em desenvolvimento e sistemas alojados em infraestruturas de terceiros de forma sistemática e consistente. A segurança da Informação do Banco é mandatada para estabelecer e manter uma cultura de segurança em todo o Banco, garantir um ambiente de controle robusto, garantindo que os requisitos das partes interessadas para a proteção de dados sejam atendidos continuamente, com foco na confidencialidade (o risco de acesso não autorizado a sistemas de dados e tecnologia), integridade (risco de manipulação de dados) e disponibilidade (risco de indisponibilidade de sistemas de dados e tecnologia quando necessário). Essa norma informa e efectiva à direção do Banco em relação a gestão da resiliência cibernética. Os princípios de gestão de resiliência cibernética de tecnologias abaixo são aplicados de maneira proporcional ao tamanho e complexidade do país membro do Grupo, unidade de negócio ou função corporativa. Caso um dos princípios abaixo não seja aplicado ao nível apropriado, os Gestores de Segurança da Informação (em conjunto com o Director de Segurança da Informação (CISO)) tem o mandato de intervir e remediar a seu critério. A framework de segurança da informação é representada no diagrama abaixo, assim como os princípios de cada componente:	which include systems in production, systems in development, and systems hosted on third-party infrastructures in a systematic and consistent manner. The Bank's Information Security is mandated to establish and maintain a culture of security throughout the Bank, ensure a robust control environment, ensure that stakeholder requirements for data protection are met on an ongoing basis, with a focus on confidentiality (the risk of unauthorized access to data systems and technology), integrity (risk of data manipulation) and availability (risk of unavailability of data systems and technology when necessary). This standard informs and makes effective the Bank's management in relation to the management of cyber resilience. The technology cyber resilience management principles below are applied in a manner commensurate with the size and complexity of the Group member country, business unit or corporate function. In the event that one of the principles below is not applied at the appropriate level, Information Security Managers (in conjunction with the Chief Information Security Officer (CISO)) have a mandate to intervene and remediate at their discretion. The information security framework is represented in the diagram below, as well as the principles of each component:

		
5.1	**Governança**	**Governance**
5.1.1	A Framework de Segurança da Informação articula como o Banco determina seus objectivos de resiliência cibernética e tolerância a riscos cibernéticos, bem como como identificar, mitigar e gerenciar riscos cibernéticos de forma eficaz.	The Information Security Framework articulates how the Bank determines its cyber resilience and cyber risk tolerance objectives, as well as how to identify, mitigate and manage cyber risks effectively.
5.1.2	A framework abrange pessoas, processos e tecnologia e alinha-se às estratégias de gestão de riscos corporativos, bem como as normas internacionais e nacionais	The framework covers people, processes, and technology and aligns with corporate risk management strategies as well as international and national standards
5.1.3	A framework define claramente as funções e responsabilidades necessárias para gerir o risco cibernético e permite a medição e o relatório precisos do estado do controlo de segurança cibernética.	The framework clearly defines the roles and responsibilities required to manage cyber risk and enables accurate measurement and reporting of the state of cybersecurity control.
5.1.4	A framework inclui a gestão de riscos cibernéticos apresentados por provedores de serviços e terceiros.	The framework includes the management of cyber risks posed by service providers and third parties.
5.1.5	A adequação da framework de segurança da informação é avaliada e medida anualmente por meio de testes e análises independentes realizados por entidades externas qualificadas.	The adequacy of the information security framework is evaluated and measured annually through independent testing and analysis carried out by qualified external entities.
5.1.6	O investimento em resiliência cibernética é apropriado em valor e priorização e está claramente articulado nos níveis relevantes da organização. O impacto de qualquer trade-off é identificado e, quando necessário, escalado.	Cyber resilience investment is appropriate in value and prioritization and is clearly articulated at the relevant levels of the organization. The impact of any trade-off is identified and, where necessary, escalated.

5.1.7	É atribuída a um executivo sénior a responsabilidade e a prestação de contas pela execução do quadro de Ciber-Resiliência. Este papel tem autoridade, independência, recursos e acesso suficientes ao conselho de administração. O executivo sénior que desempenha esta função possui a experiência e o conhecimento necessários para planear e executar com competência as iniciativas de ciber-resiliência.	A senior executive is responsible for implementing the cyber resilience framework. This role has sufficient authority, independence, resources and access to the board of directors. The senior executive in this role has the experience and knowledge to competently plan and execute cyber resilience initiatives.
5.2	**Identificação / Previsão**	**Identification / Prediction**
5.2.1	Os sistemas de suporte a operações críticas (sistemas voltados para o cliente / que afetam o cliente) são protegidos contra riscos numa ordem de prioridade.	Critical operations support systems (customer-facing/customer-affecting systems) are protected against risk in an order of priority.
5.2.2	Os sistemas críticos são determinados com base no perfil de ameaças e no risco cibernético	Critical systems are determined based on threat profile and cyber risk
5.2.3	Um inventário de activos, configurações do sistema e direitos de acesso são mantidos e revistos periodicamente.	An inventory of assets, system configurations, and access rights are maintained and reviewed periodically.
5.2.4	A resiliência cibernética leva em consideração o risco representado pelas interconexões com outros sistemas internos e externos.	Cyber resilience takes into account the risk posed by interconnections with other internal and external systems.
5.2.5	As avaliações de risco devem ser conduzidas para entender a postura de segurança e o perfil de risco para operações críticas e ativos de informação de suporte ao comissionar, fazer alterações ou descomissionamento, para proteger contra comprometimento, bem como dependências externas e determinar prioridade.	Risk assessments must be conducted to understand the security posture and risk profile for critical operations and supporting information assets when commissioning, making changes or decommissioning, to protect against compromise as well as external dependencies and determine priority.
5.3	**Protecção / Prevenção**	**Protection / Prevention**
	As seguintes práticas de ciber-higiene devem ser realizadas regularmente para manter a saúde e a segurança dos utilizadores, dispositivos, redes e dados. O objectivo da ciber-higiene é manter os dados seguros e protegê-los de roubos ou ataques. Estas práticas de ciber-higiene estão elaboradas	The following cyber-hygiene practices should be carried out regularly to maintain the health and safety of users, devices, networks, and data. The goal of cyber-hygiene is to keep data safe and protect it from theft or attack. These cyber hygiene practices are elaborated in other policies and

	noutras políticas e normas que são referenciadas nas práticas de ciber-higiene abaixo:	standards referenced in the cyber hygiene practices below:
5.3.1	**Gestão de Identidades e Acessos:** O acesso físico e lógico a aplicações empresariais, sistemas de informação, redes e dispositivos informáticos deve ser concedido com base na necessidade e em conformidade com a norma lógica de gestão do acesso. As actividades destas contas devem ser registadas e revisadas como parte da monitorização contínuo.	Identity and Access Management: Physical and logical access to business applications, information systems, networks and computing devices should be granted on a need-to-basis and in accordance with the logical access management standard. Activities of these accounts should be logged and reviewed as part of ongoing monitoring.
5.3.2	**Gestão de Acesso Privilegiado:** O acesso privilegiado ao sistema é protegido por meio de controles de autenticação forte, é limitado a colaboradores autorizados específicos e é registado para actividades maliciosas. Isso estará de acordo com o padrão de gestão de acesso privilegiado.	Privileged Access Management: Privileged access to the system is protected through strong authentication controls, is limited to specific authorized employees, and is logged for malicious activity. This will be in accordance with the privileged access management standard.
5.3.3	**Segurança de Dados:** A implementação de medidas apropriadas para prevenir e detectar o roubo de dados deve ser realizada para proteger contra modificações não autorizadas, e de acordo com a política de protecção de dados.	Data Security: Implementation of appropriate measures to prevent and detect data theft should be performed to protect from unauthorized modification, and in accordance with the data protection policy.
5.3.4	**Autenticação:** Implementação de mecanismos de autenticação apropriados para garantir que todas as identidades (utilizadores, dispositivos, sistemas e robôs) sejam validadas e de acordo com o padrão de autenticação.	Authentication: Implementation of appropriate authentication mechanisms to ensure all identities (users, devices, systems, and robots) are validated, and accordance with the authentication standard.
5.3.5	**Segurança da Rede:** A protecção da rede deve ser efetuada através da realização de controlos de segurança e da adopção de uma abordagem de defesa aprofundada, em conformidade com as normas de segurança da rede.	Network Security: Protection of the network should be performed through implementation of security controls and adopting a defence-in-depth approach, and in accordance with the network security standard.
5.3.6	**Gestão de Vulnerabilidades e Patches:** Deve ser realizada a implementação de controlos de segurança para reduzir qualquer risco colocado por vulnerabilidades para a organização.	Vulnerability and Patch Management: Implementation of security controls to reduce any risk posed by vulnerabilities to the organization should be performed.

5.3.7	**Configurações Seguras:** Os sistemas são projectados para serem resilientes a ataques cibernéticos e incidentes por meio de um conjunto escrito de padrões de segurança.	Secure Configurations: Systems are designed to be resilient to cyberattacks and incidents through a written set of security standards.
5.3.8	**Protecção contra Malware:** A implementação da protecção de endpoint para proteger contra infecções por malware e abordar canais comuns de entrega de malware deve ser executada.	Malware Protection: Implementation of endpoint protection to protect from malware infection and address common delivery channels of malware should be performed.
5.3.9	**Segurança Web:** Implementação de controlos de segurança para detectar e prevenir riscos de segurança que possam comprometer a confidencialidade, integridade e disponibilidade dos serviços e activos de informação alojados em websites, servidores web e aplicações.	Web Security: Implementation of security controls to detect and prevent security risks that may compromise the confidentiality, integrity and availability of the services and information assets that are hosted in websites, web servers and applications.
5.3.10	**Formação em Cibersegurança e Sensibilização:** Todos os funcionários recebem formação e sensibilização adequadas com base no seu perfil de risco.	Cyber Security and Awareness Training: All staff are provided with appropriate training and awareness based on their risk profile.
5.4	**Detecção**	**Detection**
5.4.1	Devem ser mantidas capacidades eficazes de ciber-resiliência para reconhecer sinais de um potencial incidente cibernético ou detectar que ocorreu um comprometimento real.	Effective cyber resilience capabilities should be maintained to recognize signs of a potential cyber incident or detect that an actual compromise has taken place.
5.4.2	Devem ser estabelecidos processos de monitorização sistemática para detectar rapidamente ciberincidentes e avaliar periodicamente a eficácia dos controlos identificados.	Systematic monitoring processes should be established to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls.
5.4.3	Os sistemas devem ser continuamente monitorizados (em tempo real ou quase em tempo real) para detectar actividades e eventos anómalos.	Systems should be continuously monitored (in real time or near real time) to detect anomalous activities and events.
5.4.4	Devem existir sistemas para monitorizar as configurações de controlo, controlar a disponibilidade e a cobertura, controlar os desvios e apoiar as actividades do mapa mundial de Segurança.	Systems should be in place to monitor control configurations, control availability and coverage, and control deviations and supports world map activities.

5.4.5	As capacidades de monitorização e detecção devem facilitar o processo de resposta a ciberincidentes e apoiar a recolha de informações para o processo de investigação forense.	Monitoring and detection capabilities should facilitate the cyber incident response process and support information collection for the forensic investigation process.
5.4.6	Esses logs devem ser protegidos contra acesso não autorizado e de acordo com o Padrão de Log de Segurança.	These logs must be protected against unauthorized access and in accordance with the Security Logging Standard.
5.4.7	Deve ser criado um centro de operações de segurança ou serviços de segurança para facilitar a monitorização e análise contínuas de cibereventos, bem como a detecção e resposta rápidas a ciberincidentes.	A security operations center or acquired managed security services should be established to facilitate continuous monitoring and analysis of cyber events as well as prompt detection and response to cyber incidents.
5.4.8	Configurar eventos ou alertas do sistema de TI para fornecer uma indicação antecipada de problemas que podem afectar seu desempenho e segurança	Configure IT system events or alerts to provide an early indication of issues that may affect its performance and security
5.4.9	Deve ser efectuada uma correlação de múltiplos eventos registados nos registos do sistema de TI para identificar padrões de actividades suspeitas ou anómalas.	Multiple events recorded in the IT system logs should be correlated to identify patterns of suspicious or anomalous activity.
5.4.10	Definir processos, funções e responsabilidades para operações de segurança.	Define processes, roles and responsibilities for security operations.
5.5	**Resposta e Recuperação**	**Response and Recovery**
5.5.1	A Segurança da Informação é o responsável pela custódia e alinhado com o BCM deverá ter planos de resposta definidos para todos os riscos cibernéticos identificados.	Information Security is responsible for custody and aligned with BCM must have defined response plans for all identified cyber risks.
5.5.2	Estabeleça políticas ou padrões e processos eficazes de gestão de incidentes que ajudarão a melhorar a resiliência, apoiar a continuidade dos negócios, melhorar a confiança do cliente e das partes interessadas e, potencialmente, reduzir qualquer impacto.	Establish effective incident management policies or standards and processes that will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.
5.5.3	Caso a retomada dos serviços não seja possível, existem planos de contingência, incluindo a reversão para processos manuais.	If resumption of services is not possible, there are contingency plans, including reverting to manual processes.

5.5.4	Os planos de resposta são testados e actualizados regularmente para incluir novas ameaças.	Response plans are regularly tested and updated to include new threats.
5.5.5	Os sistemas são projectados para facilitar a resposta a incidentes, incluindo o registo de eventos do sistema e acções do utilizador.	Systems are designed to facilitate incident response, including logging of system events and user actions.
5.5.6	Os backups de dados estão disponíveis de acordo com os objectivos de ponto de recuperação e de tempo de recuperação, incluindo dados de terceiros	Backups of data are available in line with recovery point objectives and recovery time objectives, including data at third parties.
5.5.7	Certifique-se de que todos os dados confidenciais armazenados na mídia de backup estejam protegidos (por exemplo, criptografados).	Ensure any sensitive data stored in the backup media is secured (e.g. encrypted).
5.5.8	Deve ser implementada uma estratégia de comunicação clara com os clientes e parceiros financeiros afectados por ciberataques, incluindo pormenores sobre eventuais recursos disponíveis para os clientes financeiros.	A clear communication strategy to financial customers and partners impacted by cyber-attacks should be implemented, including details on any recourse available to financial customers.
5.5.9	Deverá ser estabelecido um processo para investigar e identificar as deficiências no controlo de segurança que resultaram no comprometimento. Todas as informações recolhidas a partir da inteligência cibernética e as lições aprendidas com os incidentes cibernéticos devem ser utilizadas para melhorar os controlos de segurança existentes ou melhorar o plano de resposta e gestão de incidentes cibernéticos. Este aspecto será igualmente utilizado para informar a prioridade das iniciativas em matéria de ciber-resiliência.	A process should be established to investigate and identify the deficiencies in the security check that resulted in the compromise. All information gathered from cyber information and lessons learned from cyber incidents should be used to improve existing security controls or improve the cyber incident management and response plan. This will also be used to inform the priority of cyber resilience initiatives. initiatives.
5.6	**Capacidade de Teste**	**Testing Capability**
5.6.1	O programa de resiliência cibernética é testado anualmente para validar a sua eficácia.	The cyber resilience program is tested annually to validate its effectiveness.
5.6.2	Os testes incluem campanhas de phishing, avaliações de vulnerabilidades, criação de perfis de risco, simulações com a equipa especializada (Red Team) do Grupo e testes de penetração	Testing includes phishing campaigns, vulnerability assessments, risk profiling, simulations with the Group's Red Team, and penetration testing
5.7	**Consciência / Comunidade**	**Situational Awareness / Community**

5.7.1	As informações sobre ameaças cibernéticas são recolhidas de várias fontes para prever possíveis eventos e operações críticas (por exemplo, assinaturas de inteligência de ameaças, grupos de partilha de informações locais e globais etc.).	Cyber threat information is gathered from various sources to predict potential critical events and operations (e.g., threat intelligence signatures, local and global information-sharing groups, etc.).
5.7.2	A equipa de Segurança da Informação local recebe do Centro de Operações de Segurança Cibernética (CSOC) a informação sobre a análise de ameaças, e tem a responsabilidade de mitigar os riscos cibernéticos.	The local Information Security team receives information about threat analysis from the Cyber Security Operations Center (CSOC), and has the responsibility of mitigating cyber risks.
5.7.3	As lições apreendidas sobre informação sobre ameaças são utilizadas para definir melhorias no programa de resiliência cibernética.	The lessons learned about threat intelligence are used to define improvements in the cyber resilience program.
5.8	**Cultura**	**Culture**
5.8.1	As competências e conhecimentos de segurança são continuamente desenvolvidos para que colaboradores, clientes e parceiros acompanhem as últimas tendências tecnológicas, ferramentas e técnicas utilizadas pelos atacantes.	Security skills and knowledge are continuously developed so that employees, customers and partners keep up with the latest technological trends, tools and techniques used by attackers.
5.8.2	A ciber-resiliência consiste em medidas que utilizam métricas e modelos de maturidade adequados e baseados no risco.	Cyber Resilience is measures using appropriate risk-based metrics and maturity models.
6	**Acção Disciplinar**	**Disciplinary Action**
	A adopção dos princípios desta política é obrigatória e a não conformidade relevante será submetida ao Director de Segurança da Informação (CISO). A Negligência ou má conduta podem resultar na instauração de procedimentos disciplinares.	Adoption of the principles of this policy is mandatory, and relevant non-compliance will be submitted to the Head of Information Security (CISO). Negligence or misconduct may result in the initiation of disciplinary proceedings.
7	**Informação Relacionada**	**Related Information**
	Esta seção inclui informações relacionadas que os responsáveis pela presente norma precisam conhecer para cumprir totalmente com a mesma.	This section includes related information that those responsible for this standard need to know in order to fully comply with this standard.

Tipo	**Documento / Autoridade**	**Referência**
Norma Internacional	ISO/IEC 27001; 2013; ISO/IEC	ISO/IEC 27001 international

Type	**Document / Authority**	**Reference**
International Standard	ISO/IEC 27001;	ISO/IEC 27001 international

Norma Internacional	CPMI-IOSCO	Guidance on cyber resilience for financial
Política	Information risk policy	Group Operational Risk
Política	Logical Access Management Policy	Group Operational Risk
Playbooks	SBG Technology	SBG Technology

International Standard	CPMI-IOSCO	Guidance on cyber resilience for financial market
Policy	Information risk policy	Group Operational Risk
Policy	Logical Access Management Policy	Group
Playbooks	SBG Technology	SBG Technology

8	**Administração da Política**	**Policy Administration**
Nome: Higino João		**Name:** Higino João
Cargo: CISO		**Title:** CISO
Departamento: Segurança da Informação		**Department:** Information Security
Telefone:		**Telephone:**
Email: higino.joao@standardbank.co.ao		**Email:** higino.joao@standardbank.co.ao

9	**Histórico de Revisão**		**Revision History**	
Version no.	**Purpose of Review**	**Review date:**	**Effective date:**	**Summary of key revision points:**
V1	Desenvolvimento da Política	Abril de 2020	Abril de 2020	• Adopção da Política
V2	Revisão Anual	Fevereiro de 2022	Fevereiro de 2022	• Actualização do Responsável • Actualização da Data de Validade
V3	Revisão Anual	Junho de 2023	Junho de 2023	• Actualização do Responsável
V4	Revisão	Novembro de 2025	Novembro de 2025	• Alteração da Administração da Política • Actualização da Data de Validade da Política • Actualização da Norma para Política • Adição de Princípios Gerais • Adição novos de controlos de governança

				• Adição novos de controlos de Identificação e Previsão • Adição novos de controlos de protecção e prevenção • Adição novos de controlos de detecção • Adição novos de controlos de Resposta e Recuperação • Adicão da direcção de Segurança da Informação
V5	Revisão	Março de 2026	Março de 2026	• Adequação da data de revisão da Política