# Política de Segurança de Informação (Resumo)

# Banco BIR, S.A.

**Detalhes do documento**

| | |
|---|---|
| **Título:** | Política de Segurança de Informação (Resumo) |
| **Ficheiro:** | DSIC_Política de Segurança de Informação (Resumo) |

**Revisão do documento**

| Data: | Versão | Responsável | Motivo de intervenção |
|---|---|---|---|
| 05-2026 | V.1 | DSIC | Actualização |
| 05-2026 | V.1 | DOQ | Formatação/Verificação |
| 05-2026 | V.1 | CI | Validação |

**Aprovado por:**

| Data: | Versão | Nome |
|---|---|---|
| 28-05-2026 | V.1 | Conselho de Administração |

**Actualizações ao normativo:**

| Versão | Data de entrada em vigor | Alterações |
|---|---|---|
| V.0 | 02-04-2023 | Criação (CE.OS.001.2023) |
| V.1 | 28-05-2026 | Actualização Geral (CE.OS.001.2023) |

**Legislação/Regulação de suporte ao normativo:**

| Diploma | Data de entrada em vigor | Assunto |
|---|---|---|
| Lei nº 14/21 | 19 de Maio | Lei do Regime Real das Instituições Financeiras |
| Aviso n.º 08/20 | 02 de Abril | Política de Segurança Cibernética e Adopção de Computação em Nuvem |
| Aviso 03/2026 | 02 de Fevereiro | Sistema Financeiro - Código do Governo Societário das Instituições Financeiras |

**Abreviaturas:**

- **Banco BIR –** Banco de Investimento Rural, S.A
- **DOQ –** Direcção de Organização e Qualidade
- **C.A –** Conselho de Administração
- **C.E –** Comissão Executiva
- **U.O –** Unidades Orgânicas

## ÍNDICE

## 1. APRESENTAÇÃO

O presente documento é a versão pública da Política de Segurança de Informação do Banco BIR, S.A. ("Banco" ou "BIR"), publicada em conformidade com o Aviso n.º 08/20, de 2 de Abril, do Banco Nacional de Angola. Apresenta os princípios, o modelo de governação, os compromissos e os canais de contacto do Banco em matéria de segurança de informação. A versão integral, de carácter estritamente interno, contém os controlos técnicos que dão execução aos compromissos aqui assumidos.

A segurança cibernética é uma condição da actividade bancária. O Banco trata-a como tal, em três planos: como matéria de governação ao mais alto nível, como obrigação contínua perante os seus clientes e contrapartes, e como compromisso vinculativo perante o regulador.

## 2. PRINCÍPIOS

A actuação do Banco em segurança cibernética é orientada pelos seguintes princípios:

**Confidencialidade, integridade e disponibilidade.** O Banco protege a informação que detém ou processa contra divulgação não autorizada, alteração indevida e indisponibilidade.

**Autenticidade e responsabilização.** Toda a actuação no perímetro do Banco é imputável a sujeitos identificáveis, e o Banco preserva a capacidade de verificar a identidade dos seus utilizadores, dos seus colaboradores e das suas contrapartes.

**Abordagem baseada no risco.** Os controlos do Banco são calibrados em função do risco real, evitando tanto a sobreprotecção desproporcionada como a subprotecção de activos críticos.

**Defesa em profundidade.** A protecção não depende de um único controlo. O Banco utiliza camadas múltiplas e complementares, de modo que a falha de uma não comprometa a segurança do conjunto.

**Segurança desde a concepção.** Os requisitos de segurança são incorporados nas fases iniciais do desenho dos processos, sistemas, produtos e serviços do Banco.

**Conformidade.** O Banco cumpre integralmente o quadro regulamentar aplicável à sua actividade e aos serviços que presta.

**Melhoria contínua.** O Banco revê e actualiza periodicamente o seu modelo de segurança cibernética, em função da evolução do panorama de ameaças, dos resultados de auditorias e testes, e das lições aprendidas com incidentes.

## 3. MODELO DE GOVERNAÇÃO

A segurança cibernética é, no Banco, uma matéria de governação, e não uma matéria exclusivamente técnica.

O Conselho de Administração detém a responsabilidade última pela segurança cibernética do Banco, aprova a Política de Segurança Cibernética, e recebe informação consolidada sobre o seu estado com periodicidade trimestral.

A Comissão Executiva é responsável pela execução da Política, pela afectação dos recursos necessários, e pelas decisões executivas em matéria de tratamento de risco cibernético.

A Direcção de Segurança de Informação e Cibernética dirige a função operacional de segurança do Banco e é responsável pela proposta da Política, pela coordenação da resposta a incidentes, pela emissão de parecer técnico nas iniciativas com impacto material em segurança cibernética, e pela representação do Banco perante as autoridades competentes nesta matéria.

O Banco adopta o modelo das três linhas de defesa. As áreas de negócio e as funções de suporte protegem os activos de informação que detêm e operam, constituindo a primeira linha. A Direcção de Segurança de Informação e Cibernética, em articulação com as funções de gestão do risco operacional e de conformidade, estabelece o quadro de protecção, monitoriza o seu cumprimento e desafia as decisões de risco, constituindo a segunda linha. A auditoria interna avalia, com independência, a adequação e a eficácia das duas primeiras linhas, constituindo a terceira linha.

## 4. QUADRO REGULAMENTAR E REFERENCIAL

O Banco cumpre, em matéria de segurança cibernética, o quadro regulamentar nacional vinculativo, designadamente:

- Lei n.º 22/11, de 17 de Junho — Lei da Protecção de Dados Pessoais
- Lei n.º 23/11, de 20 de Junho — Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação
- Decretos Presidenciais n.º 256/25, n.º 258/25 e n.º 263/25 — Estratégia Nacional de Cibersegurança e respectiva arquitectura institucional
- Aviso n.º 08/20, de 2 de Abril, do Banco Nacional de Angola, sobre Política de Segurança Cibernética e Adopção de Computação em Nuvem
- Aviso n.º 3/26, de 23 de Fevereiro de 2026, do Banco Nacional de Angola, sobre Governo Societário e Sistema de Controlo Interno
- Directiva n.º 05/DSB/DRO/2022, de 2 de Junho, do Banco Nacional de Angola, sobre Gestão dos Riscos das Tecnologias de Informação e Comunicação e da Segurança Cibernética
- Directiva n.º 11/DSB/DRO/2021, de 5 de Outubro, do Banco Nacional de Angola, sobre Gestão da Continuidade de Negócio
- Instrutivo n.º 10/2020, de 29 de Maio, do Banco Nacional de Angola, sobre reporte de incidentes de segurança cibernética

Como referenciais técnicos de boas práticas, o Banco adopta a norma ISO/IEC 27001:2022, a norma ISO/IEC 27002:2022, o NIST Cybersecurity Framework (versão 2.0), e o SWIFT Customer Security Controls Framework, este último na sua qualidade de participante na rede SWIFT.

## 5. ÁREAS DE ACTUAÇÃO

### 5.1.1. Protecção da informação e dos sistemas

A informação detida ou processada pelo Banco é classificada em função da sua sensibilidade, e os controlos aplicáveis a cada classe são calibrados em conformidade. O Banco protege a confidencialidade dos dados pessoais e da informação sujeita a sigilo bancário através de controlo de acesso, autenticação reforçada, criptografia da informação em trânsito e em repouso, e mecanismos de prevenção da fuga de informação.

O acesso aos sistemas do Banco obedece aos princípios do menor privilégio. O acesso remoto, o acesso privilegiado e o acesso aos canais digitais de prestação de serviço a clientes estão sujeitos a autenticação multifactor.

O Banco implementa controlos de prevenção, detecção e resposta a software malicioso em todos os pontos do seu ambiente tecnológico susceptíveis de exposição, e mantém capacidade de monitorização contínua de eventos de segurança nos seus sistemas críticos e canais digitais.

### 5.1.2. Resposta a incidentes e resiliência

O Banco mantém um Plano de Resposta a Incidentes de Segurança Cibernética, aprovado pela Comissão Executiva, que define o regime de detecção, qualificação, contenção, erradicação, recuperação e comunicação aplicável aos incidentes que afectem os seus sistemas, serviços ou informação.

Em caso de incidente sujeito a comunicação regulamentar, o Banco comunica-o ao Banco Nacional de Angola nos termos do Instrutivo n.º 10/2020, observando os prazos e a cadência regulamentares. Comunica igualmente, na medida em que se justifique, à Agência de Protecção de Dados em caso de violação de dados pessoais, ao Centro Nacional de Cibersegurança, às autoridades de aplicação da lei em caso de indícios de prática de ilícitos criminais, e aos clientes afectados nos termos descritos na secção 6.

A segurança cibernética é parte integrante do quadro de gestão da continuidade de negócio do Banco, em conformidade com a Directiva n.º 11/DSB/DRO/2021. O Banco mantém mecanismos de cópia de segurança, recuperação e localização alternativa adequados à criticidade dos seus serviços.

### 5.2.1. Adopção de computação em nuvem

A adopção de serviços de computação em nuvem pelo Banco obedece ao disposto no Capítulo III do Aviso n.º 08/20 e demais regulamentação aplicável. Cada adopção é precedida de avaliação formal do risco associado, de parecer técnico da Direcção de Segurança de Informação e Cibernética, e de comunicação prévia ao Banco Nacional de Angola.

### 5.3.1. Participação na rede SWIFT

O Banco participa na rede SWIFT e cumpre os requisitos do SWIFT Customer Security Programme. Realiza, com periodicidade anual, a atestação de conformidade ao SWIFT Customer Security Controls Framework, submetida a asseguramento independente em conformidade com as regras da SWIFT.

### 5.3.2. Gestão de terceiros

A contratação e manutenção de relações com terceiros que envolvam acesso, processamento, armazenamento ou transmissão de informação do Banco, ou a operação dos seus activos, estão sujeitas a avaliação prévia do risco cibernético, a cláusulas contratuais de segurança proporcionais ao risco, e a monitorização contínua durante a vigência do contrato.

### 5.3.3. Cultura de segurança

O Banco promove uma cultura institucional de segurança cibernética, assente na sensibilização contínua dos seus colaboradores e na capacitação técnica das funções com responsabilidades específicas. A sensibilização de base é obrigatória para todos os colaboradores, com periodicidade anual, e abrange os princípios da Política, a classificação da informação, o uso aceitável dos recursos do Banco, o reconhecimento de tentativas de engenharia social e os deveres de comunicação de eventos de segurança.

## 6. COMPROMISSOS PERANTE OS CLIENTES

O Banco assume, perante os seus clientes, os seguintes compromissos em matéria de segurança cibernética:

**Informação sobre segurança.** O Banco disponibiliza, através do seu sítio institucional, dos seus canais digitais, das suas agências e dos seus centros de atendimento, informação clara e actualizada sobre os comportamentos seguros na utilização dos seus produtos e serviços, sobre os principais vectores de ameaça dirigidos aos clientes de instituições financeiras, e sobre os procedimentos a adoptar em caso de suspeita de fraude.

**Identificação dos canais oficiais.** O Banco identifica claramente os canais, números, endereços e identificadores oficiais que utiliza na comunicação com os seus clientes,

permitindo-lhes distinguir a comunicação legítima do Banco da comunicação fraudulenta dirigida a clientes.

**Comunicação de campanhas de ameaça.** Quando o Banco identifique campanhas de ameaça com potencial impacto material sobre os seus clientes, designadamente as que envolvam os seus canais, produtos ou identidade institucional, comunica essa informação aos clientes afectados, ou potencialmente afectados, através dos canais adequados e em tempo útil.

**Comunicação de incidentes que afectem clientes.** Em caso de incidente de segurança cibernética que afecte materialmente informação ou activos de clientes, o Banco comunica-o aos clientes afectados nos termos da regulamentação aplicável, designadamente em matéria de protecção de dados pessoais.

**Resposta a reportes dos clientes.** O Banco mantém canais formais para a recepção, qualificação e resposta a reportes de fraude e a outras situações de segurança suscitadas pelos seus clientes.

## 7. CANAIS DE CONTACTO E COMUNICAÇÃO DE EVENTOS

Para a comunicação de eventos de segurança, incluindo suspeitas de fraude, tentativas de acesso indevido e outros incidentes que afectem o cliente na utilização dos serviços do Banco, encontram-se disponíveis os seguintes canais:

- Linha telefónica de apoio ao cliente — tel: +(244) 226 461 179 / 923 125 020
- Agências do Banco — atendimento presencial em qualquer agência

Para a comunicação responsável de vulnerabilidades identificadas em sistemas, serviços ou canais do Banco por investigadores de segurança, terceiros qualificados ou utilizadores em geral, encontra-se disponível o seguinte endereço: (dsic@bir.ao).

As comunicações recebidas neste canal são tratadas com confidencialidade e processadas no quadro do processo de gestão de vulnerabilidades do Banco.

## 8. REVISÃO E ACTUALIZAÇÃO

A Política de Segurança de Informação do Banco é revista com periodicidade anual, e sempre que ocorram alterações materiais no quadro regulamentar aplicável, no perfil de risco do Banco, no panorama de ameaças ou no quadro tecnológico do Banco. A presente versão pública é actualizada em correspondência com a versão integral.