Políticas e Procedimentos de Segurança de Informação e Cibernética

Banco BIR, S.A

ÍNDICE

1. INTRODUÇÃO

O presente documento foi elaborado com base na ISO/IEC 27001, em harmonia com os requisitos regulamentares definidos pelo Aviso n.º 08/20, de 02 de Abril, referente à Política de Segurança Cibernética e Adopção de Computação em Nuvem e o Instrutivo n.º 10/2020, de 29 de Maio, sobre o Reporte de Incidentes de Segurança Cibernética. Este documento consiste no resumo do documento Políticas e Procedimento de Segurança de Informação e Cibernética, algo mais abrangente e extenso do que apenas a cibernética e os seus desafios de segurança. Com a implementação desta política vimos assegurar que o BIR garante a integridade, confidencialidade e disponibilidade da informação dos seus sistemas de informação. De igual modo, preserva a privacidade dos seus clientes e colaboradores.

2. PRINCÍPIOS GERAIS

A Política de segurança de informação e cibernética, refere-se a todos os aspectos de protecção do Banco, dos Colaboradores e activos, contra ameaças internas e externas. Tem abrangência total, sendo aplicável a todas as suas áreas de negócio, suporte e controlo, no que se refere a possíveis incidentes de segurança da informação.

Está alinhada com o plano estratégico da Instituição cujas metas são:

a) Sustentabilidade do modelo de negócio que passa, entre outros aspectos, pelo estabelecimento de protocolos com parceiros que, em determinado momento, carecerão de desenvolvimento de plataformas digitais para operacionalidade independente, além de soluções como o Confirming e Factoring.

b) Reforço das competências digitais, meta transportada para a generalidade deste documento sendo que a tendência e aposta interna é de transformação em Banco digital, aonde todas as soluções e processos são entregues ao cliente no conforto do seu espaço pessoal, remetendo para o presencial apenas processos especificamente exigíveis.

c) Crescimento sustentado na aposta em ferramentas que confiram mais mobilidade e foco no cliente.

d) Mobilização de talentos que, nada mais é do que a profissionalização através da formação e retenção dos quadros internos conferindo-lhes competências que

permitam à Instituição criar resposta interna seja de negócio ou suporte técnico.

3. PERFIL DA INSTITUIÇÃO

O Banco BIR é uma instituição de pequena dimensão, com um total de 130 colaboradores e representação física na província de Luanda por intermédio de 6 agências, 2 centros de Empresas e centros de ATM's. O modelo de negócio da Instituição passa por fazer uma banca tradicional apoiada em produtos de crédito, depósitos à ordem e a prazo e cartões de débito e de crédito internacional. Quanto ao perfil de risco é conforme relatório ICAAP, publicado pelo Banco em 2021, no site institucional.

4. PAPÉIS E RESPONSABILIDADES

Todo colaborador, independentemente do cargo, função ou local de trabalho, é responsável pela segurança das informações do Banco BIR e deve cumprir as determinações da política, normas e padrões de segurança da informação.

O papel a desempenhar e responsabilidades são distribuídas ao longo de 7 níveis definindo, inclusivamente, a responsabilidade de entidades externas que estabelecem parcerias com o Banco BIR.

5. NORMAS DE GESTÃO DE INFORMAÇÃO

Todo colaborador do Banco BIR é responsável pela segurança da informação a que tem acesso, independentemente da hierarquia ou cargo.

Toda a informação é classificada de acordo com a tipologia definida no Aviso n.º 08/20, de 02 de Abril e tem por objectivo proporcionar ao utilizador a possibilidade de analisar as suas informações, facilitando a definição do seu nível de acesso e condições de armazenamento, considerando sua confidencialidade, integridade e disponibilidade.

6. REGRAS DE ACESSO

O acesso à informação e conforme a sua classificação, é definida pelo utilizador de criação podendo ser a mesma partilhada de forma; restrita, confidencial, interna ou pública. É da total responsabilidade de quem produz/gere informação, a proteção de dados, seja de orientação interna ou de domínio publico.

7. INTEGRIDADE E DISPONIBILIDADE

A Integridade é a garantia de que o conteúdo da informação não será acedido ou alterado indevidamente. A Disponibilidade garante que os colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessário nos moldes definidos pela instituição.

8. SEGURANÇA E ACESSO DAS APLICAÇÕES

O Banco BIR garante a total segurança do seu parque tecnológico, utilizadores e acessos através de uma série de regras e medidas de controlo interno garantindo a conformidade com as melhores práticas de utilização de software licenciado, segmentação de acessos à internet e disponibilidade de ferramentas que cumpram com as necessidades dos utilizadores.

9. GESTÃO DE INCIDENTES DE SEGURANÇA

O Banco BIR possui uma política especifica e detalhada para o tratamento e mitigação de incidentes, devidamente catalogada e separada por 5 tipos de cenário. Tem, de igual modo, uma preocupação relevante com acções dos seus parceiros tecnológicos.

10. CONSCIENTIZAÇÃO PARA A CULTURA DA SEGURANÇA

É uma preocupação relevante disseminar a conscientização para a segurança de dados e informação e elaboramos acções contínuas de massificação de informação relevante, para melhoria da cultura interna dos colaboradores, desmistificação de temas relevantes e comunicação transversal externas através de cada colaborador do Banco.

11. COMPUTAÇÃO EM CLOUD

É dado o devido cumprimento ao exposto nos artigos 9.º ao 12.º do Capítulo III do Aviso n.º 08/20, de 02 de Abril no que concerne aos temas de adopção, comunicação, contratação e classificação da informação a migrar para a Nuvem.

12. AVALIAÇÃO E GESTÃO DE RISCO

Uma vez que os riscos não são estáticos, pois as ameaças ou vulnerabilidades mudam abruptamente, faz-se necessário o monitoramento constante para identificação atempada das mudanças que venham a ocorrer. Nesse capítulo, faz-se a monitorização continua de:

- Novos activos inseridos à estrutura corporativa;

- Novas ameaças que podem ocorrer de forma interna ou externa ao Banco;
- Possibilidade que novos processos venham a gerar vulnerabilidades exploráveis;
- Incidentes relacionados à segurança da informação;
- Modificação de processos existentes que possam contribuir para ameaças ou vulnerabilidades.

13. DISPOSIÇÕES GERAIS

Há todo um cuidado com a gestão de padronizações tecnológicas e acompanhamento contínuo assegurando-se assim visitas periódicas às dependências do Banco por forma a auscultar opiniões, necessidades e temas relevantes com o objectivo de melhorar a prestação de serviços na vertente interna e externa.

14. APROVAÇÃO DIVULGAÇÃO REVISÃO E ACTUALIZAÇÃO

A presente política é divulgada com linguagem clara e acessível ao público através das plataformas digitais (canais internos) do Banco, para prestadores de serviços e para os colaboradores. A política é revista anualmente ou quando algum evento o obrigue.