Política de Segurança Cibernética

Versão 2.0.

Mapa de Revisões

Número de Versão	Data	Motivo	Observações
1.0.	22-09-2022	Elaboração inicial	
2.0.	Maio de 2025	Alinhamento integral com o Aviso n.º 08/2020 e inclusão de novas secções sobre contratação de serviços em nuvem, resposta a incidentes e formação/sensibilização.	

Documento

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

Índice

1 INTRODUÇÃO

A presente política estabelece as diretrizes, controlos e procedimentos necessários para proteger os dados e os sistemas de informação do Banco Comercial do Huambo (BCH). Esta política foi desenvolvida em conformidade com o Aviso nº 08/2020, de 02 de abril, do Banco Nacional de Angola, as diretrizes SWIFT CSP, o PCI DSS bem como com normativos internacionais reconhecidos, incluindo ISO/IEC 27001, ISO 27035, NIST Cybersecurity Framework e PCI DSS.

Em conformidade com o Aviso nº 08/2020, esta política considera os seguintes aspetos essenciais:

- **Dimensão e perfil de risco:** O BCH adota um modelo de gestão de risco alinhado com as melhores práticas internacionais, aplicando métricas para identificar e classificar riscos cibernéticos.
- **Modelo de negócio:** Como instituição financeira, o BCH opera com serviços bancários digitais e físicos, abrangendo desde transações de retalho a operações de crédito e investimentos.
- **Sensibilidade dos dados:** A Instituição gere dados financeiros, pessoais e estratégicos de clientes, parceiros e colaboradores, exigindo medidas reforçadas para garantir a sua proteção.

O seu objetivo é garantir a confidencialidade, integridade e disponibilidade dos ativos de informação, protegendo os interesses do BCH, dos seus clientes, colaboradores e parceiros. Além disso, reflete o compromisso da Instituição com a implementação de medidas robustas de proteção de dados pessoais e financeiros e com o cumprimento das regulamentações aplicáveis.

2 APLICAÇÃO

A Política de Segurança Cibernética aplica-se 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 ativo de informação do Banco, nomeadamente dados, sistemas, equipamentos e infraestruturas.

As diretrizes de segurança cibernética são igualmente aplicáveis a todos os sistemas, dados e informações do Banco independentemente do seu formato, estado (armazenada, em trânsito 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 (coletiva ou singular) com quem o Banco tem uma relação profissional e contratual, para fim de atingir objetivos específicos;
c) **Parte interessada:** todos os elementos (pessoas, instituições, grupos, órgãos governamentais, etc.) que de alguma forma afetam ou são afetados pela organização.

3 DEFINIÇÕES

- **Segurança Cibernética:** Conjunto de políticas, procedimentos, controlos e tecnologias destinados a proteger redes, sistemas e dados contra acessos não autorizados e ataques digitais.
- **Computação em Nuvem:** Modelo de prestação de serviços que permite o acesso remoto a recursos computacionais e armazenamento de dados, com gestão simplificada.
- **Infra-Estrutura Tecnológica Crítica:** Sistemas e ativos de informação essenciais para a operacionalidade do Banco, cuja indisponibilidade ou destruição pode causar impactos significativos.
- **Classificação da Informação:**
    - **Muito confidencial:** Informação cuja divulgação pode causar prejuízos financeiros e de imagem graves; acesso restrito aos níveis mais altos da gestão.
    - **Confidencial:** Informação estratégica que, se divulgada, pode impactar negativamente o negócio; acesso restrito a gestores e colaboradores autorizados.
    - **Reservada:** Informação destinada a grupos específicos dentro da organização; divulgação controlada internamente.
    - **Interna:** Informação de uso interno, divulgada somente mediante autorização para o público externo.

- **Pública:** Informação que pode ser divulgada sem restrições, observando cuidados quanto à sua apresentação.

4 Princípios Fundamentais de Cibersegurança

- **Defesa em profundidade:** Implementação de camadas de segurança para reduzir riscos.
- **Confidencialidade:** Assegurar que a informação é acessível apenas a pessoas autorizadas, protegendo dados sensíveis de acessos não autorizados.
- **Integridade:** Garantir a precisão e confiabilidade da informação, prevenindo alterações não autorizadas ou corrupção de dados.
- **Disponibilidade:** Garantir que os sistemas e serviços essenciais estão operacionais e acessíveis conforme necessário.
- **Autenticidade:** Assegurar que os dados, sistemas e utilizadores são legítimos e verificáveis.
- **Responsabilidade e Auditoria:** Assegurar que todas as ações e acessos sejam monitorizados, registados e auditáveis para rastreamento e mitigação de riscos**.**
- **Gestão de riscos:** Identificação, avaliação e mitigação de cyber ameaças.
- **Zero Trust:** Minimização de privilégios e verificação contínua de acessos.
- **Cultura de segurança:** Capacitação contínua e sensibilização dos colaboradores.

5 Diretrizes e Controlos de Segurança

O Banco adota os seguintes controlos e medidas, de acordo com as melhores práticas e requisitos regulamentares:

- **Autenticação e Autorização:** Implementa mecanismos robustos para garantir o acesso seguro aos sistemas.
- **Criptografia:** Aplica criptografia para a transmissão e armazenamento de informações sensíveis.
- **Prevenção de Intrusões e Software Malicioso:** Utiliza sistemas de deteção e prevenção de intrusões (IDS/IPS) e antivírus atualizados.
- **Controlo de Acesso e Segmentação de Redes:** Define perfis de acesso e segmenta as redes para reduzir a superfície de ataque.

- **Cópias de Segurança (Backups):** Mantém backups regulares e testados, garantindo a recuperação dos dados em caso de incidentes.
- **Testes e Auditorias:** Realiza periodicamente testes de vulnerabilidade e auditorias de segurança para identificar e mitigar riscos.
- **Prevenção de Fuga de Informação:** Implementa medidas para evitar a transferência não autorizada de dados.

6 Gestão e Resposta a Incidentes

O Banco mantém um plano estruturado para deteção, contenção e resposta a incidentes de segurança cibernética. Conforme exigido pelo regulador, este plano prevê:

- **Plano de Ação e Resposta a Incidentes:** O Banco mantém um plano que define:
  - Procedimentos para o registo, análise, contenção e recuperação de incidentes;
  - Atribuição de responsabilidades para a resposta a incidentes;
  - A obrigatoriedade de notificação imediata ao Banco Nacional de Angola e, posteriormente, a cada 4 horas até à normalização dos serviços, conforme exigido pelo Aviso nº 08/2020.
- **Registo e Monitorização:** Todos os incidentes são documentados, analisados e reportados à Direção de Sistemas de Informação (DSI).

7 Contratação de Serviços de Computação em Nuvem

O BCH adota critérios rigorosos na contratação de serviços em nuvem, garantindo:

- **Avaliação e Seleção:** Antes da contratação, o BCH verifica a capacidade do prestador para assegurar a confidencialidade, integridade, disponibilidade e recuperação dos dados, bem como a conformidade com os requisitos legais e normativos.

- **Notificação ao Banco Nacional de Angola:** O BCH comunica a intenção de contratação com, pelo menos, 60 dias de antecedência, contendo:

  - Dados do prestador e localização do datacenter;
  - Plano de continuidade de negócio;

- Informações detalhadas sobre os serviços e a legislação aplicável;

- **Cláusulas Contratuais:** As cláusulas contratuais incluem obrigações de cooperação, auditoria independente, acesso a relatórios e medidas de segurança compatíveis com os requisitos do Aviso.

8 RESPONSABILIDADES

A segurança cibernética no BCH está estruturada com responsabilidades distribuídas entre diferentes níveis organizacionais para garantir a implementação eficaz desta política:

- **Órgão de Administração / Conselho de Administração**
  - Aprovar esta política, zelar pela **cultura de segurança** e disponibilizar recursos necessários.
  - Acompanhar periodicamente métricas e relatórios de segurança cibernética.
- **Equipa de Segurança Cibernética / Direção de Sistemas de Informação (DSI)**
  - Implementar e monitorizar os controlos previstos nesta política.
  - Conduzir **testes de segurança**, formações e análise de incidentes.
  - Garantir a notificação rápida de incidentes ao BNA, conforme exigência regulamentar.
- **Gestores de Área**
  - Assegurar a aplicação dos requisitos de segurança cibernética no âmbito das suas equipas.
  - Reportar à Equipa de Segurança Cibernética qualquer incidente ou anomalia.
- **Colaboradores e Parceiros**
  - Cumprir todos os procedimentos de segurança definidos.
  - Participar nas formações internas e notificar comportamentos suspeitos ou ocorrências de segurança.

9 Divulgação, Formação e Sensibilização

Para reforçar a cultura de segurança em todos os níveis e promover o envolvimento efetivo de colaboradores, parceiros e público, estabelecem-se as seguintes medidas de divulgação e formação:

- **Divulgação Interna e Externa**: A política é divulgada de forma clara e acessível a todos os colaboradores, parceiros e ao público, garantindo a transparência e o alinhamento de todos com os princípios de segurança cibernética.
- **Formação Contínua**: O BCH realiza sessões regulares de formação e sensibilização sobre segurança cibernética, adaptadas aos diferentes níveis de acesso e funções, assegurando a consciencialização e a adesão efetiva às boas práticas de proteção de dados.

10 Revisão, Monitorização e Auditoria

Para salvaguardar a eficácia e a atualidade desta política, estabelecem-se as seguintes diretrizes de revisão, monitorização e auditoria:

- **Revisão Periódica:** A política é revista anualmente ou sempre que ocorram alterações relevantes na legislação, no modelo de negócio ou no perfil de risco, assegurando a sua atualidade e eficácia.
- **Monitorização:** A eficácia dos controlos é monitorizada de forma contínua, complementada por auditorias internas e externas, permitindo a identificação atempada de vulnerabilidades e oportunidades de melhoria.
- **Aprovação:** Todas as alterações são submetidas à apreciação e aprovação do Conselho de Administração, em conformidade com os mecanismos de governance do Banco.

11 Documentos Complementares

Esta Política de Segurança Cibernética complementa e expande a Política Global de Segurança de Informação da instituição, assegurando uma aplicação coerente de princípios, diretrizes e práticas

de proteção de dados. A coordenação entre ambas as políticas contribui para a mitigação de riscos e para a proteção efetiva das informações estratégicas do Banco.

Além disso, a presente Política é suportada por outros códigos, políticas e normativos internos, nomeadamente:

- Manual de Normas de Segurança do Sistema de Informação;
- Políticas e normativos internos, que estabelecem requisitos para a proteção dos dados e informações geridas pelo Banco, abrangendo os seguintes domínios:
    - Gestão do risco da segurança da informação;
    - Gestão de incidentes de segurança cibernética;
    - Gestão de identidades e acessos aos dados, sistemas e infraestruturas;
    - Gestão de vulnerabilidades técnicas;
    - Segurança de informação em serviços na nuvem;
    - Regras e requisitos de criptografia;
    - Utilização aceitável dos sistemas de informação.
- Outros normativos internos em vigor.

12 Disposições Finais e Sanções

O não cumprimento das disposições desta política configura infração sujeita às sanções previstas na legislação e nos regulamentos internos do Banco, em conformidade com o Aviso nº 08/2020. Quaisquer dúvidas ou omissões na interpretação desta política serão dirimidas pela Direção de Sistemas de Informação (DSI) e, se necessário, pela área Jurídica.

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.