POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

InovaData

Programa de Governança e Segurança dos Dados

Eliana Oliveira	Jéssica Grácio	Maria Fialho	Rodrigo Fernandes
2240276	2240549	2240286	2240537

Mestrado em Ciência dos Dados

No âmbito de Governança e Segurança dos dados

23/01/2025

Índice

Introdução 6

1. Identificação de Iniciativas de Gestão de Dados (Business Case) 7

2. *Engagement* e Obtenção de Compromisso das Partes Interessadas 10

2.1 *Stakeholders* 10

2.2 Assegurar o compromisso das partes interessadas 11

2.3 Importância da maturidade dos dados 11

3. Definição da Estratégia 13

3.1 Alinhamento Estratégico e Aumento do Valor do Banco 13

3.2 Definição de Metas e Objetivos 15

4. Estrutura Operacional 18

4.1 Definição da Estrutura Operacional 18

4.2 Papéis e Responsabilidades 19

4.2.1 Data Governance Comité Executive 19

4.2.2 Data Steward Comité & Workgroups 20

4.3 Matriz RACI 24

5. Implementação 26

5.1 *Roadmap* 26

5.2 Gestão de mudança 27

5.2.3 Contextualização e Objetivos da Gestão de Mudança 27

5.2.2 Identificação de Impactos e Resistências 28

5.2.3 Sustentação e Objetivos 30

5.2.4 Plano de Comunicação 31

5.2.5 Plano de Formação 32

6. Metadados, Catálogo de Dados e Gestão de Dados Mestre 34

6.1 Glossário e Dicionário de Dados 34

6.1.1 Glossário de dados 34

6.1.2 Dicionário de dados 34

6.1.3 Diferenças entre um dicionário de dados e um glossário de dados 34

6.1.4 Exemplo de um glossário de dados do banco InovaData 34

6.1.5 Dicionário de dados do banco InovaData 35

6.2 Gestão de Dados Mestre 36

6.2.1 Dados Mestre e Dados de Referência 36

6.3 Metadados 37

6.3.1 Como podemos aplicar a gestão de metadados ao Banco InovaData 38

6.3.2 Estrutura para a Gestão de Metadados 38

6.3.3 Integração da Gestão de Metadados no PGSD 39
7. Segurança e Qualidade dos Dados 40
7.1 Aquisição de Frameworks 40
7.1.1 NIST Cybersecurity Framework 40
7.1.2 Cobit 40
7.1.3 ISO/IEC 27001 40
7.1.4 Quadro Nacional de Referência para Cibersegurança 41
7.2 Políticas de Segurança dos dados 41
7.2.1 Gestão de Riscos 42
7.2.2 Qualidade dos Dados 42
8. Ferramentas de Gestão de Dados e Tecnologia 43
8.1 Collibra Data Intelligence 43
8.2 Talend 43
8.3 Microsoft Power BI 43
8.4 Microsoft SharePoint 44
8.5 Implementação 44
Conclusão 46
Referências 47
Bibliografia 47
Netgrafia 47
Anexos 49
Anexo I - Estatuto do Comité de Governança de Dados - Banco InovaData 49
Anexo II – Diagrama de *Gantt – Roadmap* PGSD 51
Anexo III – Política de Metadados 52
Objetivo 52
Âmbito 52
Definições 52
Política 52
Normas de Metadados 52
Modelo de Metadados 52
Criação e manutenção de metadados 53
Garantia de qualidade 54
Publicação e acessibilidade 54
Conformidade e aplicação da lei 54
Formação e apoio 54
Revisão da política 54

Anexo IV – Dicionário de Dados 55
Anexo V – Glossário de Dados 62
Anexo VI - *framework* HESA 68
Anexo VII - Política de qualidade dos dados 73
Objetivo 73
Âmbito 73
Definições 73
Princípios da qualidade dos dados 73
Funções e responsabilidades 74
Política 74
Conformidade e auditoria 74
Formação e apoio 75
Revisão da política 75
Anexo VIII - Política de integração de dados 76
Objetivo 76
Âmbito 76
Definições 76
Princípios da qualidade dos dados 76
Normas de Integração de Dados 76
Funções e responsabilidades 76
Processo de Integração 77
Conformidade e Revisão 77
Formação e apoio 77
Revisão da política 77
Anexo IX - Políticas de Segurança dos dados 78
1. Objetivo 78
2. Âmbito 78
3. Políticas de Segurança dos Dados 78
4. Responsabilidades 79
5. Penalizações 79
6. Auditoria e Revisão 79
7. Definições 80
8. Histórico de Revisões 80

Índice de Figuras

Figura 1 – Assessment Summary 12
Figura 2 - Problemas enfrentados pelo Banco InovaData 13
Figura 3 - Objetivos Estratégicos 14
Figura 4 – Organograma do Banco InovaData 18
Figura 5 - Modelo Operacional de GD 19
Figura 6 - Diagrama de Venn dos Impactos Organizacionais 29
Figura 7 - Linha do Tempo dos Objetivos de Sustentabilidade 30
Figura 8 - Benefícios do uso de Frameworks para cibersegurança 41
Figura 9 – Segurança de dados na gestão de riscos 42
Figura 10 - Collibra 43
Figura 11 – Talend 43
Figura 12 - Microsoft Power BI 43
Figura 13 - Microsoft SharePoint 44

Índice de Tabelas

Tabela 1 - Iniciativas de Gestão de Dados 7
Tabela 2 – Responsabilidades dos Stakeholders internos 10
Tabela 3 - Responsabilidades dos Stakeholders externos 10
Tabela 4 - Metas e Objetivos 15
Tabela 5 - Data Governance Comité Executivo 19
Tabela 6 - Data Owners por Unidade 21
Tabela 7 - Data Stewards por Unidade 22
Tabela 8 - Data Custodians por unidade 22
Tabela 9 - Matriz RACI 24
Tabela 10 - Roadmap do Programa de Governança e Segurança de Dados 26
Tabela 11 - Principais Objetivos da Gestão de Mudança 28
Tabela 12 - Avaliação e Impactos 28
Tabela 13 - Estratégias de Mitigação de Resistências 29
Tabela 14 - Metas de Sustentabilidade por Prazo 30
Tabela 15 - Plano de Comunicação 31
Tabela 16 - Estrutura e Cronograma do Plano de Formação 32
Tabela 17 – Cronograma de Sessões de Formação 32
Tabela 18 - Tabela Clientes 35
Tabela 19 - Regras de Governação e de Metadados 37
Tabela 20 - Funcionalidades do Collibra 38
Tabela 21 - Funcionalidades das Ferramentas 44

Introdução

No contexto atual, caracterizado pelo crescimento exponencial da informação global, a gestão de dados tornou-se um dos principais ativos estratégicos das organizações. Este projeto foca-se no desenvolvimento e implementação de um Programa de Governança e Segurança de Dados (PGSD) para o Banco InovaData, uma instituição fictícia que enfrenta desafios reais relacionados com a qualidade, segurança, e utilização eficaz de dados. Esses desafios refletem problemas comuns no setor financeiro, como fragmentação de sistemas, dificuldades de integração e conformidade regulatória.

Ao longo deste trabalho, serão detalhados os papéis e responsabilidades, definidas estratégias para o compromisso com as partes interessadas, elaborada uma Matriz RACI, e apresentado um plano de implementação que inclua um *roadmap* claro e gestão da mudança. Além disso, o projeto incorpora a avaliação e a seleção de ferramentas adequadas para suportar o ecossistema de dados do banco, garantindo que estas permitam conformidade regulatória e que estejam alinhadas com as necessidades estratégicas e operacionais da organização.

Outro aspeto fundamental do projeto é a gestão de metadados, que inclui a criação de glossários e dicionários de dados para melhorar a consistência e a compreensão entre departamentos. O uso de *frameworks*, como os apresentados pela DAMA e pelo autor John Ladley, será fundamental para assegurar a integridade, acessibilidade e governança de metadados.

Este PGSD representa mais do que uma resposta aos desafios identificados - ele constitui um pilar estratégico para o Banco InovaData, valorizando os dados como um ativo transformador. Ao integrar governança de dados resistente, tecnologias sólidas e um compromisso com a excelência, o projeto prepara o banco para enfrentar os desafios do futuro, permitindo a tomada de decisões informadas, o crescimento sustentável e o fortalecimento da sua posição no mercado financeiro.

1. Identificação de Iniciativas de Gestão de Dados (Business Case)

Para estruturar a governança de dados no banco InovaData, foram identificadas e priorizadas iniciativas estratégicas que alinham os objetivos do banco ao impacto esperado nos resultados. A tabela abaixo apresenta as iniciativas, destacando suas prioridades, *drivers*, objetivos e atributos mensuráveis, que servirão como referência para monitorizar o progresso e garantir resultados tangíveis.

Tabela 1 - Iniciativas de Gestão de Dados

Prioridade	Driver	Objetivos	Objetivos documentados	Atributos Mensuráveis
1	Aumentar os lucros nos próximos 3 anos	• Aumentar valor das ações do banco; • Tornar o banco mais atrativo para investidores e acionistas; • Tomar decisões sobre o futuro do banco com base em dados.	• Aumentar os lucros em 20% nos próximos 3 anos; • Utilizar dados e insights em 100% das decisões de topo.	• Lucros; • Número de decisões que utiliza dados.
2	Aumentar a quota de serviços digitais	• Aumentar as vendas de serviços digitais; • Aumentar os rendimentos com serviços digitais.	• Aumentar em 10% a quota de serviços digitais financeiros; • Aumentar os lucros provenientes de produtos digitais em 30%.	• Quota de mercado; • Vendas de serviços digitais.
3	Reforçar a reputação e credibilidade no mercado financeiro	• Garantir conformidade regulatória e políticas RGPD; • Assegurar segurança dos dados dos clientes; • Garantir que não há abusos na utilização e manipulação dos dados dos clientes; • Proteger dados contra-ataques e fuga de dados.	• Ser visto como um banco de confiança por 90% dos clientes.	• Reputação do banco; • Credibilidade percebida (Inquéritos).
4	Melhorar qualidade de dados dos clientes e aumentar oportunidades de venda cruzada	• Ajudar a melhorar os relatórios e a tomada de decisão. • Assegurar a qualidade dos dados dos clientes.	• Redução em 70% do tempo que os analistas demoram a limpar e integrar dados. • Reduzir em 80% a quantidade de dados incorretos;	• Índice de qualidade dos dados; • Percentagem de vendas cruzadas face ao período anterior.

			• Aumentar em 40% a quantidade de vendas cruzadas; • Aumentar efetividade das campanhas de marketing em 25%.	• Performance de campanhas de marketing.
5	Aumentar a satisfação dos clientes	• Oferta de serviços personalizados e apoio ao cliente rápido e acessível (quer à distância, quer presencial).	• Percentagem de clientes satisfeitos acima de 85%; • Reduzir clientes insatisfeitos em 55%; • Expandir 15% da base dos clientes nos próximos 2 anos.	• Resultados dos Inquéritos de satisfação; • Número de Base de clientes.

Relativamente à prioridade das iniciativas, sendo a 1 a mais prioritária e a 5 a menos prioritária, descritas anteriormente, considerou-se os objetivos estratégicos da organização e o impacto no crescimento sustentável.

Todas estas iniciativas são importantes para os objetivos estratégicos do banco, no entanto, esta priorização reflete a necessidade de equilibrar resultados financeiros, transformação digital, confiança no mercado e satisfação dos clientes.

1. **Aumentar os lucros nos próximos 3 anos**

Os lucros de uma empresa são a principal razão da sua existência. É através deles que é capaz de se gerar valor para a comunidade onde se insere, pagar salários e responder às necessidades dos seus clientes.

O banco InovaData não é diferente, ele procura de forma constante e sustentável aumentar os seus lucros, enquanto faz cumprir com o que considera ser as suas responsabilidades sociais. Será com os lucros obtidos que o banco será capaz de pagar aos seus acionistas e investir na inovação dentro do setor financeiro.

Para alcançar estes objetivos é essencial que a empresa seja otimizada nesse sentido, isto inclui a utilização de dados, e tudo o que a sua utilização implica, para capacitar os seus colaboradores com as ferramentas para tomar decisões informadas, baseadas em dados reais e fidedignos, obtendo vantagem competitiva sobre os seus concorrentes.

2. Aumentar a quota de serviços digitais

A crescente competição com as FinTechs exige que a organização acelere a digitalização dos seus serviços, aumentando a sua quota de 30% para 60% em dois anos, reflexo da importância que o banco dá ao crescimento dos seus serviços digitais. Melhorar os canais digitais, como a página web e as aplicações móveis, é essencial para atender às expectativas dos clientes por conveniência e personalização. Com uma gestão eficiente de dados, será possível criar interfaces mais intuitivas, otimizar processos e gerar *insights* valiosos para inovação. Isso fortalecerá a competitividade, aumentará a eficiência operacional e permitirá à organização liderar no mercado de serviços digitais.

3. Reforçar a reputação e credibilidade no mercado financeiro

Reforçar a reputação e credibilidade do banco no mercado financeiro é crucial. Este é um dos principais fatores com que o banco se posiciona no mercado. Para além de ser coerente com o seu posicionamento, a credibilidade é fundamental para angariar novos clientes, reter os atuais e consequentemente alinhar o banco com regulamentos e leis, tanto nacionais, como internacionais. Para alcançar este objetivo é crucial que os dados dos clientes dos bancos estejam seguros, dificultando a fuga de dados e a superfície de ataque do banco.

Para isso, será necessário definir políticas e procedimentos, garantir que os dados estejam atualizados, seguros e sincronizados entre os diferentes sistemas do banco, em especial o CRM e o ERP, apostando na integração de dados, redução de silos e *shadow* IT, controlo de acesso a dados sensíveis, formação dos colaboradores sobre como manipular os dados dentro do regulamento em vigor e práticas éticas e colocar mecanismos que protejam estes dados de *hackers*, tanto de forma proativa, como reativa.

4. Melhorar qualidade de dados dos clientes e aumentar oportunidades de venda cruzada

A escolha de priorizar a melhoria da qualidade dos dados dos clientes é justificada pela sua importância estratégica na tomada de decisões e na geração de oportunidades de negócio. Pois, dados confiáveis reduzem o tempo dedicado à limpeza e integração, permitindo que os analistas se concentrem em análises mais relevantes. Além disso, a redução de dados incoerentes assegura maior precisão nos relatórios, que são essenciais para decisões informadas.

Políticas de governança adequadas são fundamentais para manter a consistência e a qualidade dos dados, evitando impactos negativos em vendas e campanhas. Com dados precisos, é possível aumentar as vendas e os lucros, demonstrando um impacto direto nos resultados de negócio e na competitividade da organização.

5. Aumentar a satisfação dos clientes

A priorização de iniciativas para aumentar a satisfação dos clientes é justificada pela necessidade de oferecer serviços personalizados e um bom suporte ao cliente, fatores essenciais para melhorar a experiência do cliente, mantê-los e atrair novos clientes. Uma forma eficaz de avaliar se estes objetivos estão a ser cumpridos é através da realização de inquéritos de satisfação.

Também o objetivo de expandir a base de clientes em 15% nos próximos dois anos reforça a importância de um atendimento acessível e eficiente, assegurando competitividade no mercado e alinhamento com objetivos estratégicos.

Para alcançar estes objetivos será necessário adotar práticas que permitam identificar as dores e problemas dos clientes, bem como pontos de melhoria nos serviços do banco e no apoio ao cliente. Estas práticas incluem garantir que os dados dos clientes se encontram atualizados e integrados com os diferentes sistemas do banco, medir a satisfação do cliente ao longo do seu ciclo de vida e adotar ações para fidelizar, reter e aumentar as vendas junto dos clientes existentes.

2. *Engagement* e Obtenção de Compromisso das Partes Interessadas

2.1 *Stakeholders*

Os *stakeholders* são todas as partes interessadas ou influenciadas direta ou indiretamente por uma organização, projeto ou decisão. Incluem pessoas, grupos ou organizações que têm um interesse legítimo nos resultados, operações ou impactos de uma iniciativa. Os mesmos podem ser internos (como funcionários e gestores) ou externos (como clientes, fornecedores, acionistas, reguladores e a comunidade).

Os *stakeholders* são essenciais para o sucesso de qualquer plano, especialmente em iniciativas complexas como a governança de dados, porque definem identificam e definem prioridades e expectativas que orientam os objetivos, facilitam a obtenção dos recursos necessários, sejam eles financeiros ou humanos, garantem que as ações se alinham com interesses e objetivos da organização e avaliam e mitigam potenciais riscos relacionados à resistência ou insatisfação dos restantes *stakeholders*.

Dentro dos *stakeholders* internos do projeto de governança de dados do banco InovaData podemos destacar os seguintes da tabela que segue:

Tabela 2 – Responsabilidades dos Stakeholders internos

Grupo	Responsabilidade/Descrição
Conselho de Administração	Define as estratégias globais e aloca recursos para a governança de dados.
Direção Geral (CEO)	Responsável por assegurar que a governança de dados está alinhada com a visão estratégica e operacional.
Departamento de Sistemas de Informação	Gere a infraestrutura tecnológica e lidera a implementação técnica do plano.
Equipa de Análise de Dados	Utiliza os dados para gerar *insights*, impactando diretamente as operações e decisões estratégicas e de negócio do banco.
CISO (Chief Information Security Officer)	Focado em proteger os dados e assegurar conformidade com regulamentos como o RGPD.
BU (Business Unit) de Compliance	Garante que os dados sejam geridos de forma a atender aos requisitos regulatórios dos mercados em que o banco atua e pretende expandir.
BU de Marketing	Depende da qualidade dos dados para campanhas eficazes e personalização de serviços.
BU de Atendimento ao Cliente	Enfrenta desafios devido a dados inconsistentes e não integrados que afeta diretamente a experiência do cliente.

Por outro lado, dentro dos *stakeholders* externos podemos destacar os seguintes da tabela abaixo:

Tabela 3 - Responsabilidades dos Stakeholders externos

Grupo	Descrição/Responsabilidade
Clientes	Exigem proteção dos seus dados pessoais, além de transparência e precisão nos serviços prestados.
Reguladores (e.g., Banco de Portugal)	Garantem conformidade com regulamentações específicas, fundamentais para evitar penalizações e danos reputacionais.

Fornecedores de Tecnologia	Como o fornecedor do Siebel CRM, desempenham um papel crítico na implementação de soluções integradas.
Acionistas	Exigem relatórios confiáveis e têm interesse na reputação e rentabilidade do banco.

2.2 Assegurar o compromisso das partes interessadas

Para garantir o sucesso do plano de governança de dados, é essencial criar um ambiente no qual todas as partes interessadas (*stakeholders*) compreendam os benefícios da iniciativa e sintam que o seu envolvimento é valorizado e recompensado. A inclusão dos *stakeholders* no processo de implementação não apenas reforça a adesão, mas também promove uma cultura organizacional orientada por dados (data-driven), um elemento essencial para a transformação digital do Banco InovaData.

Uma das formas de fomentar este compromisso é a realização de iniciativas de capacitação e envolvimento, como formações regulares, *workshops*, *webinars*, e a criação de um portal de governança de dados. Estes eventos devem ser adaptados para abordar as necessidades específicas dos diferentes *stakeholders*, mas com uma base comum: apresentar os benefícios tangíveis da governança de dados para a organização, como maior eficiência operacional, melhor tomada de decisões, conformidade com regulamentações e proteção contra riscos reputacionais. Por exemplo, num workshop, podem ser apresentados casos de uso práticos de governança de dados, como a integração entre o Siebel CRM e o ERP, mostrando como reduz silos de dados e melhora a personalização do atendimento ao cliente.

Além disso, é crucial implementar medidas de incentivo que vinculem o desempenho dos colaboradores às práticas de governança de dados. Uma abordagem eficaz é incorporar metas relacionadas à qualidade de dados e à adoção de políticas de governança nos prémios de desempenho individuais e de equipa. Por exemplo, o Departamento de Sistemas de Informação pode ter objetivos específicos, como alcançar 95% de dados críticos limpos e precisos até ao final de um período definido. O cumprimento dessas metas poderia ser recompensado com bonificações financeiras, reconhecimento público ou ainda através de dias extra de férias, mantendo os colaboradores motivados e interessados no sucesso do plano de governança de dados.

Outro elemento importante é a comunicação contínua dos resultados e benefícios da governança de dados. Através do portal de governança de dados, todos os *stakeholders* podem aceder a *dashboards* que mostrem indicadores de performance, como tempos de resposta reduzidos, aumento da satisfação dos clientes e conformidade com reguladores.

Por fim, para promover uma mudança sustentável, a governança de dados deve ser incorporada na cultura organizacional do Banco InovaData. Isto inclui estabelecer líderes em governança de dados em cada unidade de negócio, que atuarão como embaixadores da iniciativa, e fomentar uma mentalidade *data-driven* em todos os níveis da organização. A transformação cultural pode ser reforçada com campanhas internas que celebrem conquistas e boas práticas, criando um senso de pertença e alinhamento dentro da organização.

A adoção de uma abordagem estruturada e inclusiva, que combine capacitação, incentivos e comunicação, será essencial para garantir o compromisso dos *stakeholders* e transformar a governança de dados numa vantagem competitiva e estratégica para o Banco InovaData.

2.3 Importância da maturidade dos dados

De forma a apurar a maturidade digital do banco foi utilizada a *framework* da HESA, com a justificação da resposta a cada questão preenchidas no Anexo VI, bem como o ficheiro Excel

(Data_capability_assessment_form_2018.xlsx) original também em anexo, sendo as respostas baseadas no documento do caso de estudo. No caso de não haver provas textuais no documento da existência de certos mecanismos ou práticas, foi considerado que estas não existem na organização.

Apreciação da maturidade dos dados

Com base na análise realizada com apoio à *framework*, o Banco InovaData enfrenta desafios significativos em várias dimensões da gestão de dados, incluindo qualidade, governança, integração e utilização estratégica. A ausência de uma abordagem estruturada e formal para dominar, modelar e gerir dados reflete-se em processos reativos, dados fragmentados e dificuldades na geração de *insights* confiáveis para a tomada de decisão. Embora haja algum reconhecimento da importância dos dados, as iniciativas existentes são pontuais e carecem de um alinhamento estratégico com os objetivos organizacionais.

De acordo com os parâmetros definidos pela *framework* utilizada, o nível de maturidade dos dados é o nível 1 (reativo), que de acordo com a mesma conclui que:

Não existe uma capacidade formal de gestão de dados. Os dados são recolhidos, armazenados e tratados num contexto inteiramente operacional. Os processos empresariais são, na melhor das hipóteses, embrionários, enquanto a tecnologia tem uma utilização muito limitada. É difícil lidar com a operação e a mudança e a qualidade dos resultados não é fiável. Culturalmente, os dados não são vistos como importantes, ou mesmo compreendidos. Não há processos repetíveis para aumentar a eficiência ou reduzir os custos, não há interesse em lidar com potenciais violações de dados legais e não há estratégia ou orientação sobre a forma como a gestão de dados pode apoiar os objetivos organizacionais.

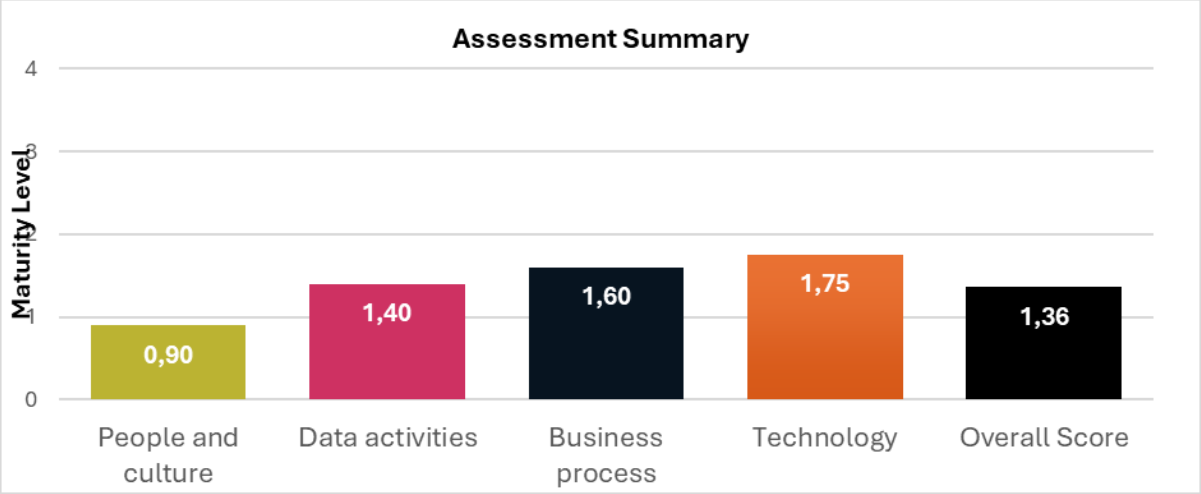


Figura 1 – Assessment Summary

O gráfico da Figura 1 representa de forma resumida a maturidade dos dados do banco. Podemos observar que todos os parâmetros se encontram ainda muito embrionários, sendo que existe uma especial deficiência ao nível das pessoas e cultura, pelo que estas deverão ser devidamente orientadas para atingir o objetivo do banco em se tornar uma empresa *data-driven*.

3. Definição da Estratégia

3.1 Alinhamento Estratégico e Aumento do Valor do Banco

A implementação de uma estratégia de governança de dados eficaz é fundamental para o Banco InovaData, especialmente devido aos desafios operacionais e estratégicos enfrentados.

Esses desafios refletem a necessidade de fortalecer a sua posição no mercado, melhorar a confiança dos clientes e aumentar a eficiência operacional. Diante desse panorama, as iniciativas propostas no Programa de Governança e Gestão de Dados (PGSD) alinham-se diretamente aos objetivos estratégicos do banco, contribuindo para a sua execução e sucesso.

De seguida, apresentam-se os principais problemas enfrentados pelo Banco InovaData (Figura 2).

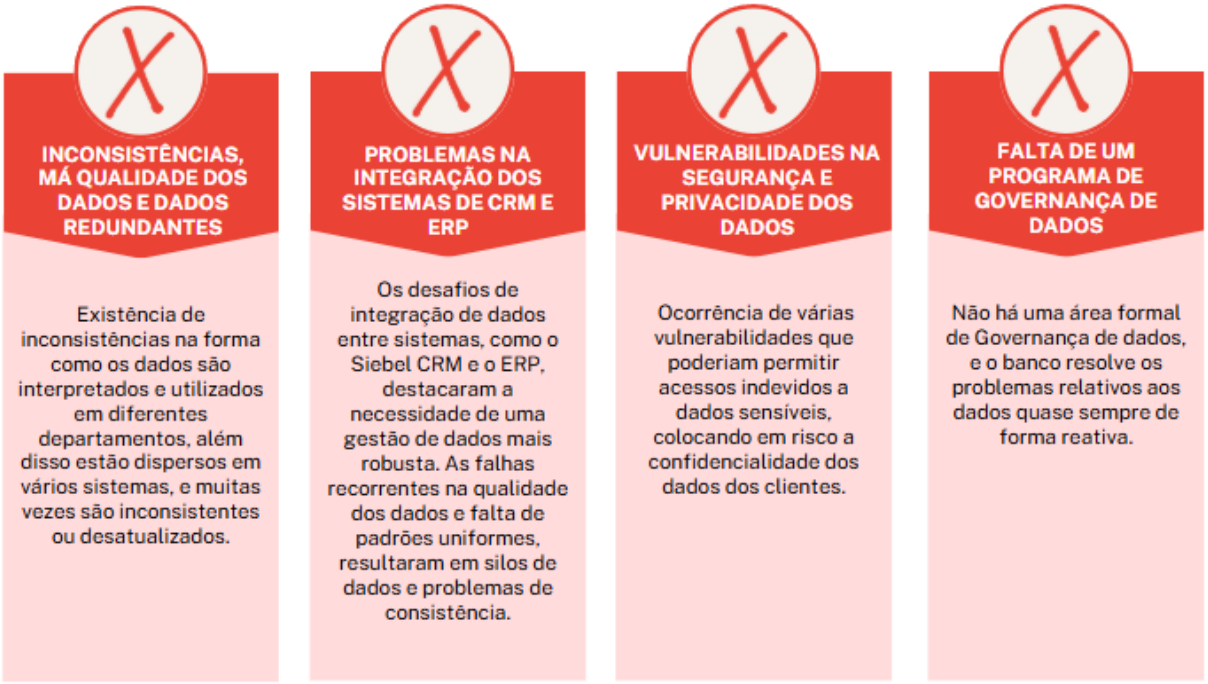


Figura 2 - Problemas enfrentados pelo Banco InovaData

Dado os problemas apresentados, é fundamental assegurar que a governança de dados não só mitigue os mesmos, mas também contribua para a melhoria contínua dos processos operacionais e estratégicos do banco.

O PGSD tem como base o desenvolvimento de capacidades estáveis de gestão de dados, como gestão de metadados, qualidade dos dados e segurança da informação. A implementação de um catálogo de dados, governança de dados e estruturação da gestão de qualidade são iniciativas fundamentais que abordam os desafios enfrentados pela organização. Além disso, essas ações estão em sintonia com a missão, visão e valores do banco, ao priorizarem a integridade, inovação contínua e foco no cliente.

Essas iniciativas apoiam diretamente os objetivos estratégicos do Banco InovaData, tais como:

Figura 3 - Objetivos Estratégicos

Além disso, o programa não apenas resolve os problemas operacionais e estratégicos, mas também gera valor tangível e intangível para a organização. Com uma estrutura de governança sólida, o banco será capaz de competir de forma mais eficaz com as *FinTechs*, garantir a confiança dos *stakeholders* e otimizar os seus processos internos.

Ao justificar estas iniciativas, fica evidente que o alinhamento estratégico proposto não só responde aos desafios enfrentados pelo banco, mas também maximiza as vantagens competitivas que um programa forte de governança de dados pode oferecer.

3.2 Definição de Metas e Objetivos

A definição de metas e objetivos é fundamental na implementação de um programa de segurança e governança de dados. As mesmas devem ser claras, pertinentes e mensuráveis. Estas devem estar alinhadas com as necessidades do banco, para garantir que o programa trará resultados concretos e significativos. Dado isto, na tabela 4 podem ser consultadas as metas e objetivos definidos para o banco InovaData, assim como as necessidades e iniciativas que as mesmas implicam.

Tabela 4 - Metas e Objetivos

Driver	Objectivos documentados	Iniciativas	Necessidades de Gestão de Dados	Capacidades DG
Aumentar os lucros nos próximos 3 anos	• Aumentar os lucros em 20% nos próximos 3 anos; • Utilizar dados e *insights* em 100% das decisões de topo.	• Implementar um Data Lake corporativo para armazenar e processar grandes volumes de dados em tempo real; • Criar relatórios e *dashboards* executivos baseados em KPIs estratégicos do banco; • Introduzir governança de dados para garantir que dados usados nas decisões sejam precisos e consistentes; • Realizar análises preditivas e cenários "what-if" para otimizar decisões financeiras; • Garantir que decisões de topo utilizem *insights* baseados em dados auditados e validados.	• Gestão de grandes volumes de dados (Big Data); • Governança de dados para decisões estratégicas; • Data Visualization and Analytics.	• Gestão de Data *Lakes*; • Governança de Dados; • Análises Avançadas e Relatórios.
Aumentar a quota de serviços digitais	• Aumentar em 10% a quota de serviços digitais financeiros; • Aumentar os lucros provenientes de produtos digitais em 30%;	• Implementar um catálogo de dados para identificar e gestão dados dos serviços digitais; • Realizar integração de dados entre sistemas para obter visão única dos clientes; • Garantir a qualidade e atualização dos dados dos produtos digitais; • Automatizar relatórios de performance dos serviços digitais;	• Gestão de metadados e integração de dados; • Qualidade dos dados; • Monitorização de desempenho; • Inteligência Artificial	• Catálogo de Dados; • Integração de Dados; • Gestão da Qualidade dos Dados.

		• Utilizar modelos de inteligência artificial para identificar potenciais clientes para serviços digitais.		
Reforçar a reputação e credibilidade no mercado financeiro	• Ser visto como um banco de confiança por 90% dos clientes.	• Implementar políticas de segurança de dados alinhadas com a RGPD, governança de dados, integração, qualidade e auditorias regulares de conformidade; • Adotar soluções de monitorização em tempo real para identificar e mitigar riscos de fuga de dados; • Criar perfis de acesso com controlos rigorosos e monitorização de uso de dados sensíveis; • Estabelecer um Comité de Governança de Dados para aprovar políticas e práticas de uso responsável dos dados; • Certificar dados críticos para decisões financeiras com processos de validação.	• Segurança e governança de dados; • Monitorização e conformidade com regulamentos; • Gestão de acessos e auditorias.	• Segurança dos Dados; • Políticas de Governança de Dados; • Controlo de Acessos e Monitorização.
Melhorar qualidade de dados dos clientes e aumentar oportunidades de venda cruzada	• Redução em 70% do tempo que os analistas demoram a limpar e integrar dados; • Reduzir em 80% a quantidade de dados incorretos; • Aumentar em 40% a quantidade de vendas cruzadas; • Aumentar efetividade das campanhas de marketing em 25%.	• Implementar uma plataforma de governança de dados com funções de validação e limpeza de dados; • Criar formações para os colaboradores; • Implementar *Data Stewardship* para melhorar o processo de gestão, governança e qualidade dos dados; • Criar processos uniformizados de integração e remover duplicação de dados dos clientes; • Aplicar análises preditivas para identificar oportunidades de venda cruzada; • Implementar *dashboards* de monitorização da performance de campanhas de marketing.	• Melhoria na qualidade e uniformização dos dados; • Gestão do ciclo de vida dos dados; • Análises avançadas e relatórios de marketing.	• Limpeza e remover duplicação de Dados; • Gestão de Dados (*Data Stewardship*) • Análise e Relatórios de Dados.

Aumentar a satisfação dos clientes	• Percentagem de clientes satisfeitos acima de 85%; • Reduzir clientes insatisfeitos em 55%; • Expandir 15% da base dos clientes nos próximos 2 anos.	• Implementar análise de dados avançada para personalizar serviços e produtos de acordo com o perfil do cliente; • Criar uma visão 360º do cliente integrando dados de múltiplos canais (web, mobile, agência); • Automatizar relatórios de satisfação do cliente para monitorizar e ajustar rapidamente os serviços oferecidos; • Introduzir um sistema de feedback em tempo real (chatbots, pesquisas digitais).; • Analisar padrões de comportamento para antecipar as necessidades dos clientes.	• Visão integrada dos dados do cliente; • Monitorização da satisfação e feedbacks; • Análise do comportamento do cliente.	• Gestão de Dados Mestre (*Master Data Management* - MDM); • Integração de Dados; • Análise de Dados em Tempo Real.

4. Estrutura Operacional

4.1 Definição da Estrutura Operacional

Para avaliar a clareza na definição da estrutura organizacional para a implementação do Programa de Governança e Segurança de Dados (PGSD) no Banco InovaData, foi considerada a divisão bem definida em *Business Units* (BUs) que abrange áreas funcionais como Finanças, Marketing, Sistemas de Informação, Atendimento ao Cliente, Compliance e Recursos Humanos.

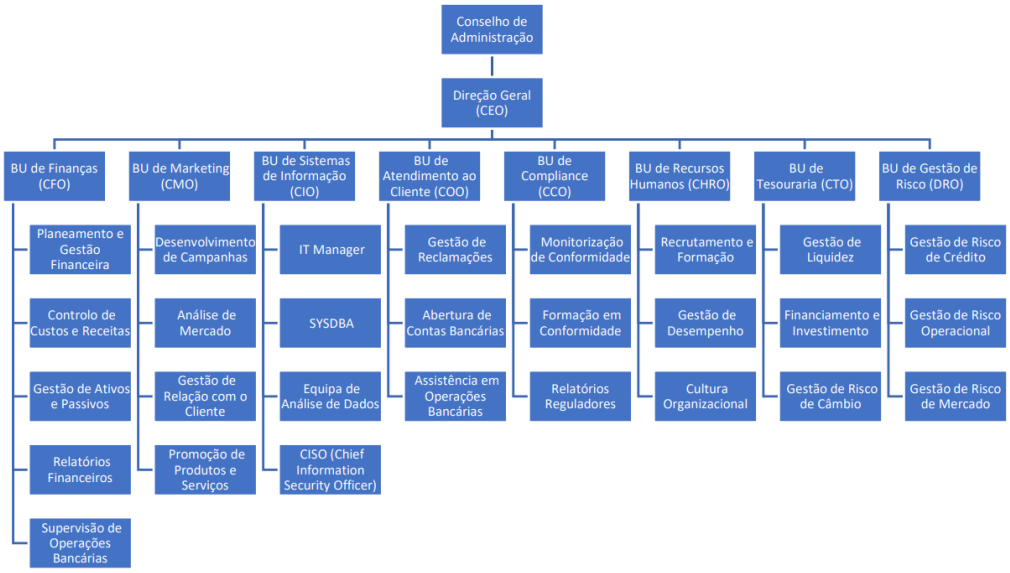


Figura 4 – Organograma do Banco InovaData

O organograma apresentado na Figura 4 ilustra a relação hierárquica e as interações entre as diferentes unidades de negócio. A estrutura é compreensível, com uma organização que reflete claramente as áreas funcionais do banco e as suas responsabilidades em termos de governança de dados.

Cada BU possui líderes identificados, como *Chief Financial Officer* (CFO), *Chief Marketing Officer* (CMO) e *Chief Information Officer* (CIO), que têm responsabilidades estratégicas alinhadas com o PGSD. Por exemplo, A BU de Sistemas de Informação, liderada pelo CIO, supervisiona a infraestrutura tecnológica e a segurança da informação, crucial para a governança de dados. Enquanto a BU de *Compliance* garante conformidade regulatória, como o cumprimento do RGPD. A descrição das suas funções indica que elas estão preparadas para apoiar a implementação do PGSD, garantindo conformidade regulatória e proteção de dados.

O Conselho de Administração e a Direção Geral têm papéis definidos de supervisão estratégica, assegurando que a implementação do PGSD seja conduzida de forma coordenada e alinhada com os objetivos organizacionais.

Com base nessas observações, a estrutura organizacional do Banco InovaData para a implementação do PGSD é clara, bem definida, e compreensível, com uma divisão explícita de responsabilidades e papéis que assegura uma organização eficiente das funções necessárias para o sucesso do programa. O modelo operacional pode ser verificado na Figura 5.

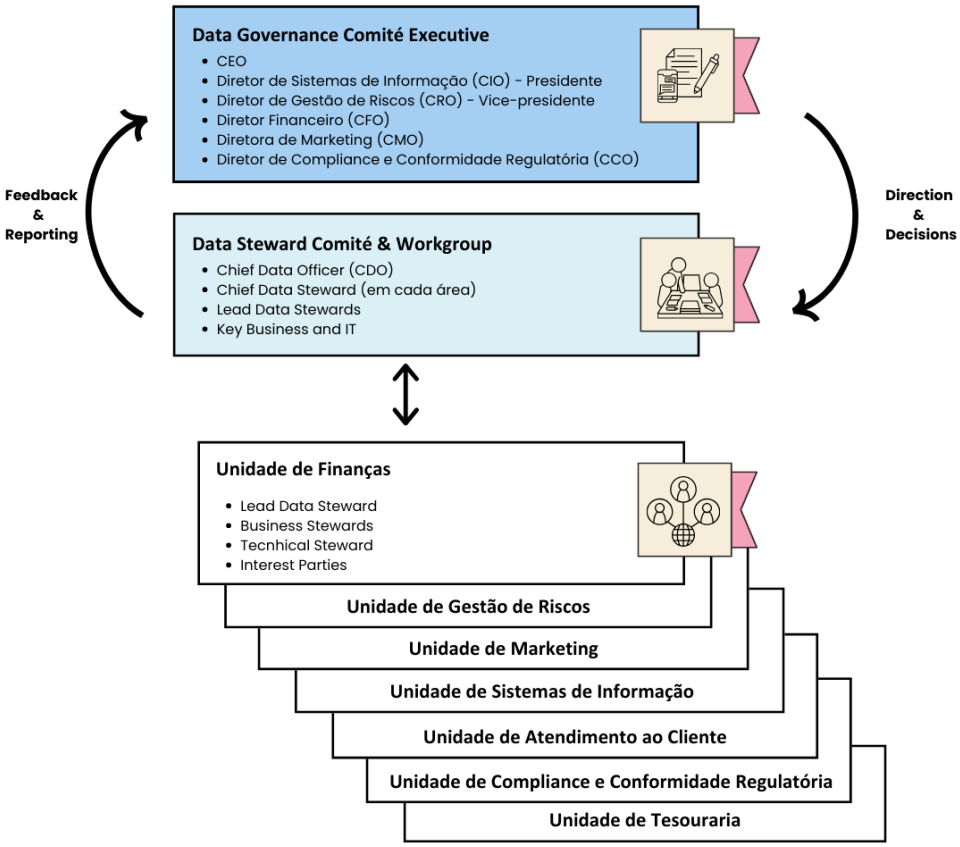


Figura 5 - Modelo Operacional de GD

4.2 Papéis e Responsabilidades

4.2.1 Data Governance Comité Executive

O Comité Executivo de Governança de Dados é responsável pela supervisão estratégica da governança de dados no Banco InovaData. Ele garante que as iniciativas de governança estejam alinhadas com os objetivos estratégicos e regulatórios do banco.

De salientar, conforme descrito no Anexo I - Estatuto do Comité de Governança de Dados, o Comité Executivo tem a autoridade formal para liderar iniciativas de governança de dados, implementar uma estrutura sólida e assegurar a qualidade, segurança e conformidade dos ativos de dados do banco. Este estatuto confere ao comité o poder de estabelecer políticas e práticas fundamentais para a governança de dados.

Os papéis e responsabilidades dos seus membros incluem:

Tabela 5 - Data Governance Comité Executivo

Posição	Responsável	Responsável
CEO	Dra. Matilde Santos	Proporciona orientação estratégica geral, assegura o alinhamento da governança de dados com os objetivos de negócios e aprova as principais iniciativas de dados.

Diretor de Sistemas de Informação (CIO) - Presidente	Dr. Pedro Alves	• Agendar e supervisionar as reuniões do Data Governance Comité Executive. • Aprovar agendas de reuniões e listas de participantes. • Garantir que a documentação, como atas e relatórios, seja preparada e distribuída. • Relatar o *status* das metas e objetivos de governança de dados. • Assegura a implementação das estratégias de TI que suportam a governança de dados.
Diretor de Gestão de Riscos (CRO) - Vice-presidente	Dr. Luís Martins	• Assumir as responsabilidades do Presidente na sua ausência.
Restantes membros: • Diretor de Gestão de Riscos (CRO) - Vice-presidente • Diretor de Finanças (CFO) • Diretora de Marketing (CMO) • Diretor de *Compliance* e Conformidade Regulatória		• Participar em todas as reuniões presencialmente ou por outro meio • Rever e fornecer contribuições sobre políticas e iniciativas. • Apoiar a implementação das práticas de governança de dados aprovadas nas suas respetivas unidades.

4.2.2 Data Steward Comité & Workgroups

Este Comité é responsável por implementar as políticas e práticas de governança de dados no nível operacional, assegurando a qualidade, consistência e segurança dos dados em toda a organização.

- **Chief Data Officer (CDO):** Coordena o programa de governança de dados, assegurando a execução das políticas de governança em todas as áreas de negócios e TI. Serve como ponte entre o Comité Executivo e os *Data Stewards*.
- **Chief Data Steward (em cada área):** Supervisiona os *Lead Data Stewards*, garantindo que as melhores práticas de qualidade e integridade dos dados são seguidas em sua área específica.
- **Lead Data Stewards:** Responsáveis pela execução das práticas de governança de dados dentro de suas áreas de competência, garantindo a qualidade e a conformidade dos dados usados nas operações diárias.
- **Key Business and IT:** Colaboram com os *Data Stewards* para garantir que as necessidades de dados das áreas de negócios e TI são atendidas, ajudando na resolução de problemas e na melhoria contínua dos processos de dados.

4.2.2.1 Data Owners, Data Stewards e Data Custodians

A implementação eficaz da governança de dados no Banco InovaData depende da clara definição e atribuição de papéis e responsabilidades. Cada unidade de negócio desempenha um papel crucial na gestão e proteção dos dados, garantindo a sua qualidade, integridade e segurança.

Os *Data Owners*, *Data Stewards*, e *Data Custodians* são fundamentais para essa estrutura, cada um com funções específicas que complementam a estratégia geral de governança de dados.

Abaixo estão detalhados os papéis e responsabilidades atribuídos a cada unidade, alinhados com suas funções operacionais e estratégicas:

Os *Data Owners* são responsáveis pela gestão geral dos dados dentro da organização, garantindo que os dados sejam utilizados de forma estratégica e que cumpram os requisitos de negócios e regulatórios.

Tabela 6 - Data Owners por Unidade

Data Owners	Unidade	Responsabilidade
Dr. João Ferreira	Unidade de Finanças (CFO - Diretor Financeiro)	Responsável pela gestão financeira e pelas decisões estratégicas relacionadas a ativos, passivos, relatórios financeiros e operações, possui autoridade sobre os dados financeiros. Ele define políticas, assegura que os dados são utilizados corretamente e conforme as normas, e supervisiona a sua aplicação.
Dr. Luís Martins	Unidade de Gestão de Riscos (CRO - Chief Risk Officer):	Responsável por garantir que os dados relacionados com os riscos financeiros e operacionais (como risco de crédito e de mercado) sejam geridos de forma eficaz, com ênfase na qualidade e conformidade regulatória.
Eng.ª Marta Soares	Unidade de Marketing (CMO - Chief Marketing Officer)	Responsável pelos dados dos clientes, em especial os dados utilizados para campanhas de marketing, vendas cruzadas e personalização dos serviços oferecidos. Deve garantir que os dados estejam alinhados com os objetivos de negócios, como a segmentação correta e a tomada de decisões informadas.
Dr. Pedro Alves	Unidade de Sistemas de Informação (CIO - Chief Information Officer)	Responsável por assegurar que todos os dados sejam acessíveis, bem geridos e seguros, permitindo uma tomada de decisão baseada em dados precisos e confiáveis.
Eng.ª Clara Rodrigues	Unidade de Atendimento ao Cliente (COO - Chief Operating Officer)	Responsável pelos dados de interações e operações com clientes. Define políticas para garantir que os dados dos clientes são utilizados corretamente nas operações de atendimento e suporte.
Dr. António Costa	Unidade de Compliance e Conformidade Regulatória (CCO - Chief Compliance Officer)	Gere os dados de conformidade, assegurando que todas as operações estão em conformidade com as regulamentações aplicáveis. Define políticas para a recolha e uso de dados regulatórios.
Dr. Luís Santos	Unidade de Recursos Humanos (CHRO - Chief Human Resources Officer)	Supervisiona os dados de colaboradores, incluindo recrutamento, formação e gestão de desempenho. Define políticas de gestão de dados de RH, assegurando a conformidade com as normas de privacidade e segurança.

Dr. André Ribeiro	Unidade de Tesouraria (CTO - Chief Treasury Officer)	Responsável pelos dados de liquidez e gestão de risco de câmbio. Define políticas para o uso e proteção desses dados, assegurando a conformidade regulatória e a eficiência operacional.

Os *Data Stewards* são os responsáveis pela administração e governança diária dos dados, garantindo a qualidade, integridade e conformidade dos dados de acordo com as políticas internas e regulatórias.

Tabela 7 - Data Stewards por Unidade

Data *Stewards*	Unidade	Responsabilidade
Chief Data Steward	TI e Infraestrutura de Dados	Responsável pela qualidade e integridade dos dados técnicos e colabora com outras áreas para garantir a implementação eficaz das políticas de governança de dados.
Chief Data Steward	Atendimento ao Cliente	Garante a qualidade e precisão dos dados de interações com clientes, assegurando o uso correto nas operações bancárias.
Chief Data Steward	Finanças	Responsável pelos dados financeiros, assegurando que os relatórios e análises são baseados em dados precisos e conformes.
Chief Data Steward	Gestão de Riscos	Responsável pela qualidade dos dados de riscos, garantindo que sejam utilizados de forma eficaz para mitigar riscos.
Chief Data Steward	Marketing	Responsável pelos dados de marketing e campanhas, assegurando precisão e conformidade para análises e personalização.
Chief Data Steward	Compliance	Responsável pelos dados regulatórios, garantindo a conformidade com as regulamentações e padrões internos.
Chief Data Steward	Recursos Humanos	Responsável pela qualidade dos dados de RH, assegurando a precisão dos dados de colaboradores e processos de RH.

Os *Data Custodians* são responsáveis pelo armazenamento, manutenção e proteção dos dados em sistemas e infraestruturas tecnológicas. Eles têm um papel operacional e de suporte técnico, garantindo que os dados sejam mantidos de acordo com os requisitos organizacionais e regulatórios.

Tabela 8 - Data Custodians por unidade

Data Custodians	Unidade / Subunidade	Responsabilidade
Dr. Pedro Alves	Unidade de Sistemas de Informação (CIO - Chief Information Officer)	Como *Data Custodian*, a Unidade de Sistemas de Informação é responsável pela infraestrutura física e tecnológica onde os dados são armazenados e

		processados. O CIO garante que os dados sejam corretamente geridos e que a infraestrutura esteja segura e acessível.
Eng. Rui Pereira	IT Manager	Gere a infraestrutura de TI, garantindo continuidade dos serviços e segurança dos dados armazenados.
Eng. Sofia Teixeira	SYSDBA	Administra bases de dados, garantindo sua integridade, segurança e acessibilidade.
Dr. Manuel Silva	CISO (Chief Information Security Officer)	Como *Data Custodian*, o CISO assegura que todos os dados, especialmente dados sensíveis, sejam armazenados de forma segura, protegidos de acessos não autorizados e cumpram com os regulamentos de proteção de dados (como o RGPD).

4.3 Matriz RACI

A Matriz RACI é uma ferramenta essencial para garantir a clareza nas responsabilidades e a correta comunicação entre os envolvidos em processos, especialmente em iniciativas complexas como a implementação do PGSD (Programa de Governança e Segurança de Dados). Na tabela seguinte é apresentada a Matriz RACI, considerando os diferentes processos e fases do PGSD dentro do banco. Esta matriz define claramente quem é Responsável (R), quem deve Aprovar (A), quem deve ser Consultado (C) e quem deve ser Informado (I).

Tabela 9 - Matriz RACI

Fase	Processo/Funções	Chief Data Officer (CDO)	Chief Data Stewards	Dr. Pedro Alves (CIO)	Dr. Luís Martins (CRO)	Dr. Manuel Silva (CISO)	Dr. António Costa (CCO)	Eng.ª Marta Soares (CMO)	Eng. Sofia Teixeira (SYSDBA)	Dr. Luís Santos (CHRO)	CEO / Board de Diretores
Planear	Identificar os canais e dados necessários para construir a visão 360º do cliente e preparar o sistema de monitorização da satisfação.	A	C	A	I	C	I	R	C	I	C
Definir	Estabelecer um Data Governance Comité Executive responsável pela supervisão estratégica da governança de dados e garantir que as iniciativas de governança estejam alinhadas com os objetivos estratégicos e regulatórios do banco	C	C	R	C	I	I	I	I	I	C
	Estabelecer um Data Steward Comité & Workgroup responsável por implementar as políticas e práticas de governança de dados no nível operacional, assegurando a qualidade, consistência e segurança dos dados em toda a organização.	R	A	A	I	I	I	I	I	I	C

	Definir políticas de segurança de dados alinhadas ao RGPD, governança de dados, integração, qualidade e auditorias regulares de conformidade.	A	A	I	I	R	I	I	I	I	C
	Analisar soluções de monitorização em tempo real para identificar e mitigar riscos de fuga de dados.	A	A	I	I	R	I	I	I	I	C
Implementar	Realizar integração de dados entre sistemas para obter visão única dos clientes.	A	R	A	I	I	I	I	A	I	C
	Criar processos uniformizados de integração e de duplicação de dados dos clientes.	A	C	A	I	I	I	I	R	I	C
	Implementar uma plataforma de governança de dados, incluindo catálogo de dados, validação, limpeza e processos de Data *Stewardship* para garantir a qualidade e gestão eficiente.	A	R	A	C	C	C	C	A	I	C
Manter	Atualizar os relatórios e *dashboards* regularmente para refletir mudanças nos KPIs ou necessidades das equipas.	A	R	A	A	A	A	A	A	I	C
	Realizar auditorias regulares e ajustes contínuos para garantir que a plataforma atenda às necessidades do banco a longo prazo.	A	R	A	A	A	A	A	A	I	C
	Criar formações para os colaboradores	R	A	I	I	I	I	I	I	C	C

5. Implementação

A implementação do programa exige um plano estruturado que inclua ações de curto, médio e longo prazo. Este capítulo apresenta o *roadmap* do programa, em que detalha as fases de implementação, alinhadas às prioridades estratégicas do banco. Também aborda a Gestão de Mudança, essencial para mitigar resistências e garantir a adoção bem-sucedida de novas políticas, processos e tecnologias.

O *roadmap* descreve como as atividades serão realizadas, prazos e entregas esperadas. Já o plano de Gestão de Mudança detalha estratégias para lidar com os impactos nas equipas, garantindo uma transição eficaz.

5.1 *Roadmap*

O *roadmap* do Programa de Governança e Segurança de Dados foi criado para guiar a implementação do programa de forma clara e organizada, em que abrange as fases de curto, médio e longo prazo. O plano define as atividades principais e os respetivos responsáveis, com um cronograma detalhado e fácil de acompanhar. Entre as ações mais importantes estão a criação de políticas de segurança, a integração de sistemas e a implementação de um *Data Lake* corporativo, que são fundamentais para garantir uma gestão de dados eficiente e sustentável.

Na tabela 10, são detalhas as atividades definidas no *roadmap*, incluindo as fases, responsáveis, prazos e prioridades, proporcionando uma visão clara das ações necessárias para alcançar os objetivos do PGSD.

Tabela 10 - Roadmap do Programa de Governança e Segurança de Dados

Grupo	Fase	Atividade	Início	Término	Duração	Prioridade
Governança e Estruturação Inicial	Curto Prazo	Estabelecer um Comité de Governança de Dados.	Jan-25	Feb-25	31	Alta
Governança e Estruturação Inicial	Curto Prazo	Implementar um catálogo de dados e definir os dados mestre, para identificar e gerir os dados do banco.	Jan-25	Mar-25	59	Alta
Qualidade e Segurança dos Dados	Curto Prazo	Implementar políticas de segurança alinhadas ao RGPD e auditorias regulares.	Jan-25	Jun-25	151	Alta
Governança e Estruturação Inicial	Curto Prazo	Implementar *Data Stewardship* para melhorar a qualidade dos dados.	Feb-25	Apr-25	59	Alta
Integração e Monitorização	Curto Prazo	Realizar integração de dados entre sistemas para obter visão única dos clientes.	Feb-25	Jul-25	150	Alta
Qualidade e Segurança dos Dados	Curto Prazo	Criar perfis de acesso com restrição de utilização de dados sensíveis.	Mar-25	Jun-25	92	Média
Cultura e Adaptação Organizacional	Curto Prazo	Criar formações para os colaboradores.	Mar-25	Aug-25	153	Baixa
Qualidade e Segurança dos Dados	Médio Prazo	Certificar dados críticos para decisões financeiras com processos de validação, incluindo a gestão de metadados.	Jul-25	Dec-25	153	Média
Integração e Monitorização	Médio Prazo	Automatizar relatórios de performance dos serviços digitais.	Jul-25	Dec-25	153	Média
Relatórios e *Insights* Estratégicos	Médio Prazo	Realizar análises preditivas e cenários "what-if" para decisões financeiras.	Jul-25	Dec-25	153	Média

Análise e Personalização Baseadas em Dados	Médio Prazo	Criar uma visão 360º do cliente integrando dados de múltiplos canais.	Aug-25	Dec-25	122	Alta
Análise e Personalização Baseadas em Dados	Médio Prazo	Aplicar análises preditivas para identificar oportunidades de venda cruzada.	Aug-25	Dec-25	122	Média
Cultura e Adaptação Organizacional	Médio Prazo	Introduzir um sistema de feedback em tempo real (chatbots, pesquisas digitais).	Sep-25	Dec-25	91	Média
Sustentabilidade e Longo Prazo	Longo Prazo	Garantir que decisões de topo utilizem insights baseados em dados auditados.	Jan-26	Dec-26	334	Alta
Sustentabilidade e Longo Prazo	Longo Prazo	Implementar um Data Lake corporativo para grandes volumes de dados.	Jan-26	Dec-26	334	Alta
Relatórios e *Insights* Estratégicos	Curto Prazo	Criar relatórios e *dashboards* executivos baseados em KPIs estratégicos.	Feb-26	Jun-26	120	Média

A fase de curto prazo concentrou-se em atividades fundamentais para estruturar a base da governança de dados, como a criação de um catálogo de dados, a implementação de políticas de segurança alinhadas ao RGPD e a constituição do Comité de Governança de Dados. Estas ações iniciais garantiram um ambiente seguro e organizado, permitindo que os dados sejam geridos com maior precisão e eficiência.

A fase de médio prazo focou-se em expandir a capacidade operacional do programa, com iniciativas como a criação de uma visão 360º do cliente através da integração de sistemas, a automatização de relatórios e a aplicação de análises preditivas para identificar oportunidades de negócio. Estas ações permitirão ao banco aumentar a personalização dos serviços e melhorar a experiência do cliente, enquanto otimizam processos internos.

Por fim, a fase de longo prazo centrou-se na consolidação das iniciativas, com destaque para a implementação de um *Data Lake* corporativo e a garantia de que decisões estratégicas fossem tomadas com base em dados auditados e validados. Este esforço assegurou a sustentabilidade do programa e a capacidade do banco de inovar continuamente.

Após a descrição detalhada das atividades no *roadmap* na tabela anterior, o Anexo II - Diagrama de Gantt - R*oadmap* PGSD apresenta uma visão visual e cronológica das fases de implementação. Este diagrama ilustra os prazos, as durações e as prioridades de cada atividade, permitindo compreender como as etapas se relacionam e quais ações devem ser realizadas em paralelo ou sequencialmente. A legenda identifica as diferentes prioridades atribuídas, garantindo que o foco seja dado às ações mais críticas para o sucesso do programa.

5.2 Gestão de mudança

5.2.3 Contextualização e Objetivos da Gestão de Mudança

A gestão da mudança é essencial para garantir que as transformações propostas no Programa de Governança e Segurança de Dados sejam bem-sucedidas e sustentáveis. Este capítulo apresenta os principais elementos do plano de gestão da mudança, em que aborda os objetivos, as estratégias de diminuição de resistências, o plano de comunicação e formação, bem como as ações para monitorização e sustentação das mudanças implementadas. Nesse contexto, a gestão da mudança destaca-se como um elemento crucial para o sucesso do programa, exigindo alterações significativas nos processos, nas tecnologias utilizadas e no

comportamento dos colaboradores. Assim, torna-se fundamental assegurar que essas mudanças sejam bem compreendidas e aceites por todos os envolvidos.

Os desafios enfrentados pelo banco, que incluem questões relacionadas à integração de sistemas, qualidade dos dados e conformidade regulatória, já foram descritos no capítulo 3.1 deste relatório. Esses desafios reforçam a necessidade de um plano estruturado de gestão da mudança, com foco em minimizar resistências e promover a adoção de novas práticas.

Os objetivos da gestão da mudança para o banco InovaData são:

Tabela 11 - Principais Objetivos da Gestão de Mudança

Objetivo	Descrição
Envolver as partes interessadas	Garantir que todos compreendam a importância das mudanças e estejam alinhados com os objetivos.
Identificar e superar resistências	Antecipar obstáculos e implementar estratégias para os ultrapassar.
Apoiar a adoção de novas práticas	Facilitar a transição para novos processos, políticas e ferramentas.
Preparar as equipas	Oferecer formação e suporte para assegurar competências adequadas.
Assegurar a sustentabilidade	Monitorizar o progresso e reforçar as boas práticas para manter as mudanças no longo prazo.

Com este plano de gestão da mudança, o banco terá as ferramentas necessárias para ultrapassar os desafios e alcançar os benefícios esperados, como maior eficiência, melhor qualidade de dados e conformidade regulatória.

5.2.2 Identificação de Impactos e Resistências

A implementação do Programa de Governança e Segurança de Dados envolve mudanças que afetam diretamente pessoas, processos e tecnologia no banco. Estas mudanças requerem uma análise cuidadosa dos principais impactos organizacionais e das possíveis resistências que podem surgir durante a transição.

A Tabela 12 apresenta uma avaliação inicial dos impactos esperados em cada uma destas dimensões, identificando desafios críticos que deverão ser endereçados para assegurar o sucesso do programa.

Tabela 12 - Avaliação e Impactos

Dimensão	Impactos Identificados
Processos	• Redefinição de fluxos de trabalho para incluir governança de dados.; • Ajustes em políticas internas para conformidade com o RGPD.
Pessoas	• Necessidade de novas competências em literacia de dados; • Resistência inicial devido à falta de compreensão dos benefícios da mudança.
Tecnologia	• Integração de novos sistemas, como o *Data Lake*; • Atualizações de segurança e infraestrutura tecnológica.

Os impactos identificados estão interligados e influenciam diretamente as dimensões de Pessoas, Processos e Tecnologias. O Diagrama de Venn abaixo ilustra estas interseções e destaca áreas críticas que requerem atenção para assegurar uma implementação bem-sucedida.

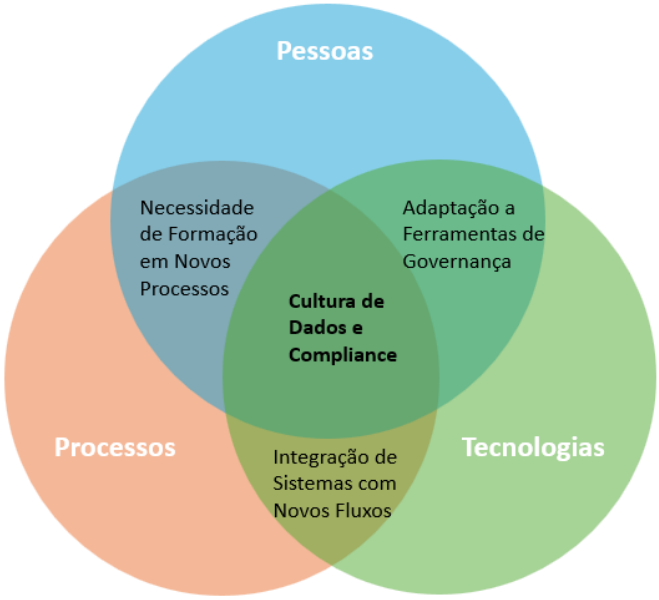


Figura 6 - Diagrama de Venn dos Impactos Organizacionais

Para lidar com estes desafios de forma estruturada e assegurar uma transição bem-sucedida, foram desenvolvidas estratégias de mitigação específicas, descritas na Tabela 13. Estas estratégias têm como objetivo abordar os problemas identificados, promover a aceitação, alinhamento e sustentabilidade das mudanças implementadas.

Tabela 13 - Estratégias de Mitigação de Resistências

Estratégia	Objetivo	Ação
Sessões de esclarecimento	Reduzir incertezas e resistências, promovendo compreensão dos benefícios da mudança.	Organizar *workshops* e reuniões explicativas com exemplos práticos sobre os impactos positivos.
Participação dos líderes de cada área	Garantir apoio e disseminação da mudança através de líderes chave em cada área.	Preparar os líderes com formação sobre o programa, fornecendo materiais de suporte como FAQs.
Formação contínua para as equipas afetadas	Preparar os colaboradores para a utilização de novas ferramentas, processos e políticas.	Desenvolver formações específicas (básico, avançado e técnico) para diferentes perfis.
Monitorização do progresso e feedback contínuo	Garantir que as resistências estão a ser superadas e que os objetivos da mudança estão a ser alcançados.	Realizar avaliações regulares com métricas específicas e recolher feedback dos colaboradores.

Motivação dos colaboradores	Garantir que os colaboradores se sentem motivados para executar o programa.	Definir objetivos por equipa e caso sejam alcançados atribuir recompensas, por exemplo bónus salarial.

5.2.3 Sustentação e Objetivos

A sustentabilidade das iniciativas de transformação organizacional depende de um planeamento bem definido e orientado por metas claras em diferentes horizontes temporais. No contexto do Programa de Governança e Segurança de Dados (PGSD), foram definidos objetivos estratégicos para curto, médio e longo prazo, acompanhados de ações concretas para garantir o sucesso do programa.

A Tabela 14 apresenta os objetivos de sustentabilidade organizados por horizonte temporal, as principais ações, resultados esperados e indicadores de sucesso para monitorizar o progresso. Estes elementos são fundamentais para assegurar que a implementação não apenas alcance os objetivos imediatos, mas também promova a integração das práticas de governança de dados na cultura organizacional.

Tabela 14 - Metas de Sustentabilidade por Prazo

Horizonte Temporal	Objetivos de Sustentabilidade	Ações Principais	Resultados Esperados	Indicadores de Sucesso
Curto Prazo	Garantir adesão inicial e execução das formações.	Realizar sessões de formação para 80% dos colaboradores.	80% das equipas treinadas em boas práticas e novas ferramentas.	Percentagem de colaboradores formados.
Médio Prazo	Reduzir resistências e consolidar as mudanças nos processos.	Rever processos e políticas internas para alinhamento ao RGPD.	Adoção de novos processos com menor resistência por parte das equipas.	Número de políticas atualizadas e aceites.
Longo Prazo	Integrar a governança de dados como parte da cultura organizacional, promovendo sustentabilidade e inovação.	Implementar o *Data Lake* corporativo e consolidar os fluxos de dados.	Governança incorporada no ADN organizacional, com maior eficiência nos processos.	Percentagem de processos alinhados à governança.

A Figura 7 complementa esta abordagem, ilustrando a linha do tempo com os objetivos principais em cada horizonte temporal. Esta representação gráfica fornece uma visão geral clara e sequencial do caminho a ser percorrido, destacando os marcos críticos que suportam a transformação organizacional.

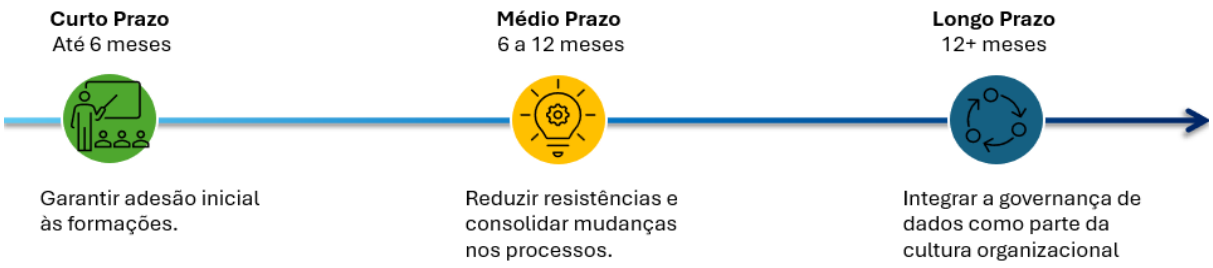


Figura 7 - Linha do Tempo dos Objetivos de Sustentabilidade

5.2.4 Plano de Comunicação

A comunicação é essencial para o sucesso do Programa de Governança e Segurança de Dados. Este plano foi criado para garantir que as informações sejam transparentes e cheguem a todos os envolvidos, promovendo alinhamento, reduzir as dúvidas e incentivar a aceitação das mudanças.

A Tabela 15 apresenta os principais objetivos e ações do plano, com foco em quem será comunicado, como será feito e com que frequência.

Tabela 15 - Plano de Comunicação

Objetivo	Mensagem Principal	Público-Alvo	Meio de Comunicação	Responsável	Frequência	Feedback
Apresentar o projeto PGSD	Introduzir os objetivos, benefícios e impacto do projeto.	Todos os colaboradores	Apresentações gerais, e-mail institucional	Equipa de Comunicação	Lançamento inicial	Inquéritos iniciais para avaliar compreensão.
Explicar mudanças específicas	Detalhar os processos e ferramentas que serão alterados.	Equipa operacional e gestores	Workshops, manuais de instruções	Recursos Humanos e TI	Mensal - durante a implementação	Perguntas e respostas em sessões de workshop.
Reforçar a importância da mudança	Sensibilizar para a governança de dados como vantagem competitiva.	Liderança e gestores	Relatórios, reuniões de alinhamento	Liderança e PMO	Trimestral	Relatórios de progresso com notas dos gestores.
Garantir alinhamento contínuo	Manter todos atualizados sobre o progresso e próximos passos.	Todos os *stakeholders*	Newsletter, portal intranet	Equipa de Comunicação	Quinzenal	Acessos ao portal e leitura da *newsletter*.
Recolher feedback	Identificar dúvidas e preocupações para ajustes contínuos.	Colaboradores de todas as áreas	Formulários online, reuniões presenciais	Equipa de Comunicação	Bimestral	Recolha e análise de sugestões enviadas.
Destacar sucessos alcançados	Compartilhar histórias de sucesso e boas práticas.	Todos os *stakeholders*	E-mails comemorativos, eventos internos	Comunicação e Recursos Humanos	Ao atingir marcos importantes	Avaliação de satisfação sobre os resultados alcançados.

O plano de comunicação garante que todos os envolvidos estejam informados e alinhados com os objetivos do PGSD. Com estratégias claras e canais de comunicação adequados, pretende-se promover a adoção das mudanças, recolher opiniões para melhorias e assegurar o sucesso do projeto através de uma comunicação eficiente e contínua.

5.2.5 Plano de Formação

O plano de formação foi desenvolvido com o objetivo de garantir que todas as equipas envolvidas estejam devidamente capacitadas para atender às exigências do programa de Governança de Dados. Para isso, o plano contempla três níveis de formação: básico, avançado e especializado. Cada nível é cuidadosamente estruturado para abranger diferentes necessidades, em que proporciona uma abordagem progressiva e alinhada aos objetivos estratégicos do programa.

As sessões de formação foram organizadas de forma a atingir públicos-alvo específicos, com responsáveis claramente designados e metas mensuráveis definidas. Este planeamento assegura uma implementação eficaz, garantindo que cada equipa receba as competências necessárias para o sucesso da governança de dados.

Tabela 16 - Estrutura e Cronograma do Plano de Formação

Nível	Descrição
Básico	Introdução à governança de dados.
Avançado	Uso de ferramentas específicas, como o *Data Lake*.
Especializado	Auditoria e análise de conformidade.

Tabela 17 – Cronograma de Sessões de Formação

Atividade	Nível	Público-Alvo	Cronograma	Descrição	Responsável	Feedback
Introdução à Governança de Dados	Básico	Todos os colaboradores	Mar-25	Sessões gerais com exemplos práticos e casos de sucesso.	Equipa de Governança	Questionários para avaliar a compreensão inicial.
Utilização do *Data Lake*	Avançado	Áreas operacionais	Mar-25 a Jun-25	Formação técnica e prática para o uso eficiente do *Data Lake*.	Especialistas de TI	Avaliações práticas ao final de cada módulo.
Auditoria de Dados	Especializado	Equipas de conformidade	Abr-25 a Jun-25	Formações focadas em processos regulatórios, validação de dados e criação de relatórios.	Equipa de Conformidade	Validação de relatórios criados durante a formação.

Workshops de Sustentação	Reforço contínuo	Gestores e áreas operacionais	Pós-implementação	Workshops periódicos para atualização de conhecimento, novas práticas e ferramentas emergentes.	Equipa de Governança e TI	Sessões de feedback para identificar lacunas de conhecimento.

O plano de formação foi criado para garantir que todas as equipas estejam preparadas para aplicar e manter as práticas de governança de dados. As atividades foram organizadas para atender às necessidades de cada grupo, a ajudar a cumprir os objetivos do programa. Além disso, o feedback recolhido durante as sessões será usado para melhorar as formações e garantir que sejam úteis e eficazes.

6. Metadados, Catálogo de Dados e Gestão de Dados Mestre

6.1 Glossário e Dicionário de Dados

6.1.1 Glossário de dados

Um glossário de dados é um repositório centralizado que reúne definições uniformizadas de termos e conceitos utilizados numa organização. A implementação de um glossário de dados é fundamental para a governança eficaz dos dados, pois ajuda a evitar ambiguidades e mal-entendidos, garantindo que os dados sejam utilizados de forma correta e eficiente. Além disso, facilita a comunicação entre diferentes departamentos e alinha a terminologia utilizada na organização.

6.1.2 Dicionário de dados

Por outro lado, um dicionário de dados é um repositório centralizado que contém informações detalhadas sobre os elementos de dados utilizados ou capturados num sistema de informação, base de dados ou projeto de investigação. Este repositório inclui nomes, definições e atributos dos elementos de dados, descrevendo os seus significados e propósitos no contexto de um projeto, além de fornecer orientações sobre a sua interpretação e representação.

A principal função de um dicionário de dados é fornecer uma linguagem comum e uma compreensão uniforme dos dados, incluindo o seu significado e as relações entre diferentes elementos de dados. Isto facilita a comunicação entre os membros de uma equipa e assegura a consistência e a qualidade dos dados utilizados. Além disso, um dicionário de dados fornece metadados sobre os elementos de dados, como os seus tipos, estruturas e restrições de segurança. Esta documentação detalhada ajuda os utilizadores e administradores a compreender melhor os dados e a garantir a sua correta utilização e gestão.

6.1.3 Diferenças entre um dicionário de dados e um glossário de dados

A diferença entre um glossário de dados e um dicionário de dados está principalmente no nível de detalhe e na finalidade de cada um. O glossário de dados é uma ferramenta mais conceptual e destina-se a definir e esclarecer os termos e conceitos do negócio relacionados com os dados. O seu foco é proporcionar uma compreensão comum dos conceitos e facilitar a comunicação entre as diferentes áreas da organização, principalmente entre equipas técnicas e não técnicas. O glossário contém definições acessíveis de termos como "Cliente", "Produto" ou "Receita", com o objetivo de garantir que todos na organização utilizem a mesma terminologia, evitando ambiguidades e mal-entendidos.

Por outro lado, o dicionário de dados é mais técnico e detalhado, sendo uma ferramenta essencial na gestão de bases de dados e sistemas de informação. Para além da definição de termos, inclui metadados, ou seja, dados sobre os próprios dados, como nomes de tabelas, campos, tipos de dados (texto, inteiro, decimal), restrições de integridade (como chave primária ou chave estrangeira) e outros aspectos técnicos importantes. O dicionário de dados é utilizado por profissionais de TI, como administradores de bases de dados e programadores, para garantir que os dados sejam armazenados e acedidos de forma consistente e eficiente. Em resumo, o glossário foca-se na terminologia e na comunicação clara dos conceitos de dados dentro do contexto do negócio, enquanto o dicionário de dados detalha as especificações técnicas dos elementos de dados dentro de um sistema.

6.1.4 Exemplo de um glossário de dados do banco InovaData

No anexo V é possível consultar um Glossário de Dados mais extenso dos principais termos para o caso de estudo do banco InovaData. Vale a pena ressaltar a existência do glossário de dados do World Bank [5], um dos principais bancos internacionais, que é bastante completo e pode ser adotado, complementado e adaptado pelo banco InovaData, sendo que possibilitaria a obtenção de vantagens como a utilização de uma linguagem mais

transversal ao setor e facilitação da adoção por novos colaboradores familiarizados com bancos que utilizam este glossário.

A seguir, segue um excerto de parte do glossário de dados do banco InovaData, pelo que uma versão mais complete pode ser consultada no Anexo V – Glossário de Dados.

A

Análise de Dados: Uso de dados estruturados e não estruturados para gerar insights que suportem decisões estratégicas.

Análise de Risco: Avaliação de potenciais perdas financeiras associadas a empréstimos, investimentos ou outros fatores operacionais.

B

Big Data: Conjuntos massivos de dados gerados e processados pela organização para obter insights estratégicos.

Base de Dados Relacional: Estrutura de armazenamento de dados organizada em tabelas interconectadas por relações lógicas.

6.1.5 Dicionário de dados do banco InovaData

A Tabela 18 faz parte do Dicionário de Dados, do sistema Core Banking. É possível consultar o dicionário de dados mais completo no Anexo IV – Dicionário de Dados.

Tabela 18 - Tabela Clientes

Clientes					
Nome do Campo	**ID_cliente**	**Nome_cliente**	**Numero_identificacao**	**Endereco**	**Informacoes_contato**
Descrição	Identificador único do cliente.	Nome completo do cliente.	Número de identificação do cliente (exemplo: número de cartão de cidadão, CPF).	Endereço completo do cliente.	Informações de contato do cliente (telefone, email, etc.).
Tipo de Dados	VARCHAR	VARCHAR	INTEGER	VARCHAR	VARCHAR
Tamanho	-	255	20	500	255
Formato	"C" seguido de número sequencial (ex: "C1", "C2", "C3", ...)	-			
Valor padrão	Criado de forma automática	-			
Valores Permitidos	Qualquer valor, desde que cumpra as restrições tipo e formato de dado exigidos				
Restrições	Chave primária, único	Obrigatório	Único, obrigatório	Obrigatório	Obrigatório

Exemplo de Valor	C1, C2, C3, C4	João Silva	123456789	Rua Principal, 1	joao@email.com, 123-456-789
Notas Adicionais	Utilizado para distinguir clientes no sistema.	-	Pode ser o número do cartão de identificação nacional, NIF ou outro dado identificador único legalmente válido.	Inclui rua, número, cidade, código postal.	Pode incluir múltiplos meios de contato separados por vírgula.

6.2 Gestão de Dados Mestre

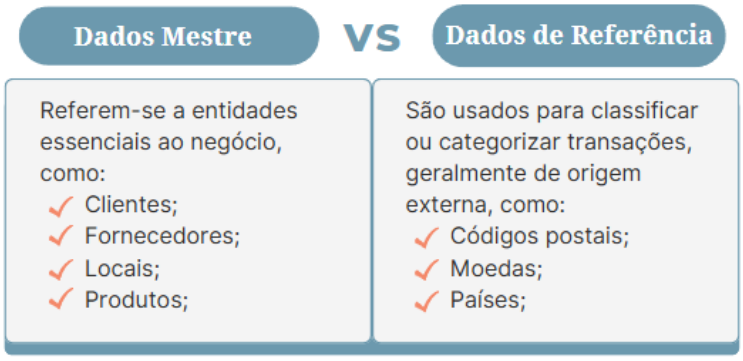
A gestão de dados mestre, ou *Master Data Management* (MDM), é um tipo específico de Gestão de Dados que consiste em identificar os elementos-chave de informação de uma empresa e depois gerir estes dados que servem como uma única fonte de verdade confiável e que consolida informações-chave, como clientes, produtos, fornecedores e locais. Normalmente estes dados não sofrem alterações em função do tempo (ou muito poucas).

A implementação de um sistema de MDM é fundamental para garantir consistência, reduzir redundâncias e melhorar a qualidade e a confiabilidade dos dados em toda a organização, contribuindo diretamente para aspetos como:

- Qualidade e Consistência: Reduz as inconsistências e a duplicação de dados.
- Decisões Informadas: Fornecer uma visão única e confiável para decisões estratégicas.
- Eficiência Operacional: Melhorar a integração entre sistemas e processos internos.
- Conformidade Regulamentar: Facilita o cumprimento de exigências legais, ao garantir a precisão dos dados.

6.2.1 Dados Mestre e Dados de Referência

Embora relacionados, os dados mestre e os dados de referência possuem diferenças importantes:



Ambos são fundamentais para as operações, mas os dados mestre têm impacto direto e central no funcionamento da organização.

As ferramentas de MDM são essenciais para implementar uma gestão eficaz de dados mestre, oferecendo recursos como:

- Integração de Fontes: Unificar dados de diferentes sistemas.
- Aplicação de Regras de Negócio: Garantir a conformidade e a consistência dos dados.

- Segurança e Proteção: Controlar acessos e proteger informações sensíveis.
- Enriquecimento de Dados: Complementar dados com fontes externas.

Exemplos de ferramentas de MDM incluem Informatica MDM, Talend, Stibo Systems e IBM Cloud Pak for Data, que oferecem soluções completas para validar e gerir dados mestre em organizações.

6.3 Metadados

Metadados são informações que descrevem outros dados, fornecendo detalhes como origem, estrutura, contexto e características dos dados principais. O prefixo "meta" vem do grego e significa "além de", indicando que os metadados vão além dos dados em si para oferecer um conhecimento mais aprofundado.

No contexto de um plano de governança e segurança dos dados, os metadados desempenham um papel central ao fornecer informações detalhadas sobre os dados que permitem a sua gestão, uso seguro e conformidade com normas regulatórias. Atuam como uma camada informativa que descreve o conteúdo, a origem, os acessos, os controlos aplicados aos dados, a forma como devem ser tratados, o seu propósito e como se encaixam nas políticas organizacionais, sendo fundamentais para sustentar estratégias eficazes de governança e segurança.

As regras de governação e de metadados normalmente incluem:

Tabela 19 - Regras de Governação e de Metadados

Regras	Descrição
Classificação e categorização de dados	Refere-se ao processo de organização dos dados com base no seu tipo, sensibilidade e importância. Por exemplo, os dados podem ser classificados como públicos, confidenciais ou restritos. A categorização pode envolver o agrupamento de dados em domínios ou assuntos específicos, tornando-os mais fáceis de gerir e localizar.
Data lineage	Mostra o percurso dos dados desde a origem até ao destino. Fornece uma representação visual da origem dos dados e da forma como se movem através dos sistemas. Isto é crucial para compreender como os dados são processados, transformados e consumidos numa organização. Ajuda a encontrar os erros até à sua origem e garante a integridade dos dados.
Métricas de qualidade dos dados	Garantem a exatidão e a fiabilidade dos dados. Estas métricas avaliam o estado dos dados. Podem avaliar a exatidão, integridade, atualidade e consistência dos conjuntos de dados. Ao monitorizar estas métricas, as organizações podem garantir que os seus dados são fiáveis e adequados para utilização.
Medidas de segurança e privacidade dos dados	Trata-se de protocolos e estratégias, como a encriptação e as auditorias regulares, implementados para proteger os dados contra o acesso não autorizado e roubo. As medidas de privacidade garantem que os dados pessoais e sensíveis são tratados em conformidade com os regulamentos e as normas éticas.
Utilização de dados e controlos de acesso	Diz respeito às permissões e restrições definidas sobre quem pode aceder e modificar os dados. Os controlos de acesso podem ser baseados em funções, o que significa que apenas funções específicas (como gestores ou analistas) têm permissão para ver

	ou editar determinados conjuntos de dados. Isto garante que os dados só estão acessíveis a quem tem permissão e protege contra alterações acidentais ou maliciosas dos dados.

6.3.1 Como podemos aplicar a gestão de metadados ao Banco InovaData

Para fazer a gestão de metadados no caso prático do Banco InovaData podemos recorrer a diversas ferramentas, tais como glossários de dados e dicionários de dados (exemplificado no ponto anterior), software dedicado para a função, através da aplicação de políticas de gestão de metadados e através da aplicação da ISO/IEC 11179 que estabelece um conjunto de normas e práticas reconhecidas internacionalmente.

6.3.1.1 - ISO/IEC 11179

A norma ISO/IEC 11179 é uma referência fundamental para a criação e gestão de metadados em organizações complexas.

Esta sugere uma abordagem de "Registo de Metadados" que inclui a identificação de atributos identificadores únicos aos elementos de dados, definição e contextualização onde se define um nome claro e descritivo para cada metadado e contexto de utilização, classificação, onde se organizam os metadados em categorias hierárquicas para facilitar a sua consulta e a qualidade para garantir que os metadados sejam precisos, atualizados e compreensíveis.

Quando aplicamos a ISO/IEC 11179 recebemos vantagens concretas na medida em que passa a existir uma uniformização dos metadados entre sistemas heterogéneos (CRM, ERP, etc.), redução de ambiguidade nos relatórios e processos e o suporte à integração dos sistemas através de um glossário e de um dicionário de dados, exemplificado no ponto anterior.

6.3.2 Estrutura para a Gestão de Metadados

Para garantir a documentação adequada de todas as fontes de dados, é fundamental desenvolver uma abordagem sistemática para a gestão de metadados que inclui o catálogo e glossário de dados (aplicados no ponto anterior) e o ciclo de vida dos metadados que inclui as etapas de criação, onde se documenta novos metadados ao introduzir novos sistemas ou fontes, a etapa de manutenção, onde ocorre uma manutenção contínua dos metadados para refletir mudanças nos sistemas e/ou processos, a etapa de acesso, onde se deve restringir o acesso aos metadados, garantindo que apenas as partes interessadas têm acesso aos dados de que necessitam e a etapa de eliminação, na qual se definem políticas para arquivo ou remoção de metadados desatualizados.

A gestão dos metadados do Banco InovaData será alcançada com recurso ao software Collibra, que irá fornecer uma estrutura de gestão de metadados, assegurando a sua correta aplicação e aderência. O Collibra é a ferramenta que irá permitir ao Banco InovaData aplicar:

Tabela 20 - Funcionalidades do Collibra

Funcionalidades	Descrição
Data Catalog	Criar um catálogo de dados centralizado para os dados e metadados, documentando a sua origem, destino e transformação.
Data lineage	Mapear visualmente o percurso dos dados através dos sistemas do banco, identificando como os dados são transformados e utilizados.

Gestão de qualidade	Monitorizar a conformidade e integridade dos dados com base nos metadados documentados, tendo em conta a política de qualidade de dados (Anexo VII).
Governança colaborativa	Promove a colaboração entre equipas, garantindo que todas as partes possam aceder e contribuir para a gestão de metadados.
Definição de políticas	O software suporta a definição e monitorização de políticas de qualidade e conformidade de dados, bem como políticas de metadados (Anexo III) e integração de dados (Anexo VIII), que deverão ser suportadas por um documento físico com o conhecimento de todos os colaboradores, assegurando que estes conhecem e entendem as suas responsabilidades no que toca aos metadados.
Auditorias e relatórios	Simplifica a criação de relatórios de conformidade, reduzindo erros e atrasos.
Monitorização	O Collibra permite ainda implementar mecanismos de monitorização para garantir a integridade e acessibilidade dos metadados, com alertas para problemas como inconsistências ou falta de conformidade.

6.3.3 Integração da Gestão de Metadados no PGSD

O Collibra será integrado com os atuais sistemas do banco (como o CRM, Core Banking, entre outros garantindo a sincronização e atualização de metadados entre sistemas e centralizando os diferentes processos e metadados.

Para o sucesso da gestão de metadados será ainda necessário alocar uma equipa dedicada, liderada por um data *steward*, com a responsabilidade de fazer a manutenção do repositório de metadados, bem como um embaixador que deve garantir que as pessoas estão a "bordo" da iniciativa e que esta está a ser executada com sucesso.

7. Segurança e Qualidade dos Dados

No contexto atual, onde os dados são considerados um ativo estratégico, a segurança e a qualidade das informações desempenham um papel crucial para o sucesso do banco. Este, enfrenta múltiplos desafios, quer na proteção de dados sensíveis e na integridade e disponibilidade dos mesmos, como na qualidade dos dados.

Para resolver estes problemas é fundamental implementar medidas de controlo de dados que sejam eficientes, pois apenas dessa forma é possível controlar e proteger informações sensíveis, para que estas sejam geridas de forma segura e alinhadas às necessidades do banco e em conformidade com os regulamentos de privacidade e confidencialidade.

7.1 Aquisição de Frameworks

Para garantir a confidencialidade, integridade e disponibilidade dos dados, é necessário adotar *frameworks* de cibersegurança que forneçam uma abordagem sistemática para gerir riscos e implementar controlos de segurança eficazes, alguns exemplos de *frameworks* para esta finalidade são, por exemplo, o *NIST Cybersecurity Framework,* o *COBIT*, a *ISO/IEC* 27001, o Quadro Nacional de Referência para Cibersegurança (QNRCS) entre outros. Abaixo pode ler-se uma breve introdução dos exemplos mencionados.

7.1.1 NIST Cybersecurity Framework

É uma ferramenta altamente adotada para proteger infraestruturas críticas contra ameaças informáticas. Esta *framework* é composta por cinco funções principais:

1. Identificar: Define e classifica os ativos de dados, avalia os riscos e determina as vulnerabilidades que podem comprometer a segurança dos dados.
2. Proteger: Implementa medidas de proteção, como criptografia, autenticação multifatorial e controlos de acesso para garantir que apenas utilizadores autorizados possam aceder aos dados.
3. Detetar: Desenvolve mecanismos de monitorização para identificar atividades suspeitas e incidentes de segurança.
4. Responder: Estabelece planos e processos para responder rapidamente a incidentes de segurança, minimizando o impacto na organização.
5. Recuperar: Define estratégias de recuperação, incluindo *backups* e planos de continuidade de negócios, para restaurar dados em caso de perda ou corrupção.

7.1.2 Cobit

O *COBIT* (*Control Objectives for Information and Related Technologies*) é uma *framework* focada em governança e gestão de TI que ajuda as organizações a alinhar as práticas de segurança com os objetivos estratégicos do negócio, garantindo que os dados sejam protegidos de acordo com as necessidades empresariais.

Esta destaca a importância de gestão de riscos, controlo de acesso e segurança da informação, fornecendo uma abordagem estruturada para a implementação de controlos de segurança e a avaliação do desempenho das práticas de segurança da organização. Esta sugere que a segurança de dados seja uma prioridade, e deve ser alinhada aos objetivos da organização e às necessidades regulatórias.

7.1.3 ISO/IEC 27001

A *ISO/IEC* 27001 é uma norma internacional que fornece diretrizes para a implementação de sistemas de gestão de segurança da informação. Ela detalha um conjunto de controlos específicos que devem ser adotados pelas organizações para proteger dados sensíveis contra ameaças. A norma abrange aspetos como controlo de acessos, auditoria, criptografia e backup, garantindo que os dados sejam protegidos, geridos e recuperados de

maneira eficaz. A implementação destas normas ajuda a garantir a conformidade com regulamentações de segurança e a adotar práticas para proteger dados sensíveis.

7.1.4 Quadro Nacional de Referência para Cibersegurança

O QNRCS apresenta um conjunto de recomendações para que as organizações possam definir uma estratégia que envolva toda a sua estrutura. As entidades podem aderir de forma voluntária e beneficiar de uma abordagem homogénea que promove uma resposta nacional a ataques informáticos. Este permite às organizações reduzir o risco associado a esses ataques, disponibilizando as bases para que qualquer entidade possa cumprir os requisitos mínimos de segurança das redes e sistemas de informação. O documento em causa reflete a realidade organizacional portuguesa, respondendo à necessidade de implementar medidas de Identificação, Proteção, Deteção, Resposta e Recuperação contra ameaças que colocam em causa a segurança do espaço digital.

Estas ferramentas não apenas ajudam a mitigar riscos, mas também melhoram a qualidade e segurança dentro da organização, facilitando a tomada de decisões baseada em dados confiáveis e bem estruturados. Apesar de funcionarem de maneira distinta e puderem divergir um pouco na sua aplicação, todas estas *frameworks* partilham vantagens em comum como as que constam na Figura 8.

Figura 8 - Benefícios do uso de Frameworks para cibersegurança

Contudo, a escolha da melhor *framework* depende das necessidades específicas, perfil de risco e setor da organização. Há alguns fatores a ter em consideração tais como:

- Dimensão da organização;
- Tipo de dados tratados;
- Requisitos Regulatórios;
- Orçamento.

7.2 Políticas de Segurança dos dados

No contexto da governança de dados, as políticas de segurança de dados desempenham um papel crucial não só como medidas de proteção contra ameaças externas, mas também como ferramentas essenciais para garantir a qualidade dos dados e para a gestão de riscos. O alinhamento dessas políticas com as boas práticas recomendadas no DAMA-DMBOK(*Data Management Body of Knowledge*) assegura que os dados sejam tratados de forma segura, íntegra e em conformidade com os objetivos organizacionais.

As políticas de segurança de dados estão descritas no Anexo IX. Estas devem ser aplicadas em todas as fases do ciclo de vida dos dados, para garantir que os mesmos estejam sempre protegidos de acordo com as necessidades da organização e as exigências regulatórias.

7.2.1 Gestão de Riscos

A gestão de riscos está intimamente ligada à segurança dos dados. Ataques informáticos, falhas de sistemas e erros humanos são alguns dos problemas que podem comprometer os dados de uma organização. As políticas de segurança de dados são um dos principais mecanismos de mitigação de riscos, segundo o DAMA-DMBOK.

A Figura 9 representa como a segurança de dados contribui para a gestão de riscos:

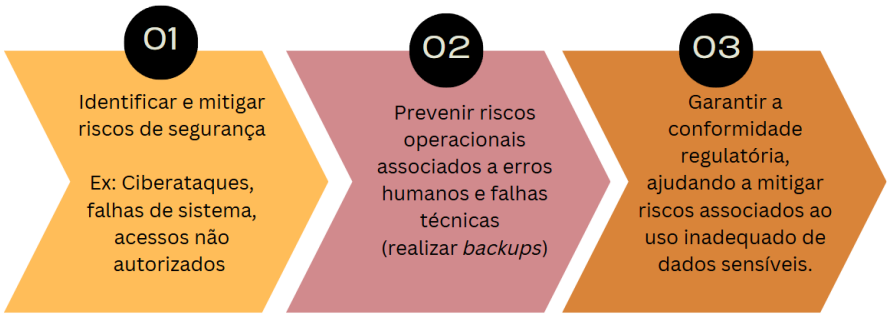


Figura 9 – Segurança de dados na gestão de riscos

7.2.2 Qualidade dos Dados

Também a qualidade dos dados é essencial para garantir que a informação utilizada pela organização seja precisa, confiável e consistente. Para que os dados mantenham a sua qualidade ao longo do tempo, é necessário protegê-los contra alterações indevidas e corrupção. Por esse motivo, as políticas de segurança de dados implementadas (Anexo IX) pretendem assegurar a qualidade dos dados, ao garantirem a proteção dos mesmos, para que estes não sejam modificados de maneira não autorizada, pois dados inconsistentes ou corrompidos podem impactar negativamente a tomada de decisões e comprometer os objetivos organizacionais.

Dado isto, podemos concluir que a implementação de *frameworks* de cibersegurança e a definição de políticas de segurança de dados são procedimentos essenciais para proteger informações sensíveis e garantir a sua qualidade e integridade. Através delas, as organizações conseguem mitigar riscos e alinhar as suas práticas de segurança às necessidades regulatórias e estratégicas assegurando uma boa qualidade de dados.

8. Ferramentas de Gestão de Dados e Tecnologia

Para resolver os principais problemas enfrentados pelo banco no âmbito do PGSD, foram selecionadas quatro ferramentas. Estas ferramentas foram escolhidas pela sua capacidade de abordar problemas específicos relacionados à qualidade, integração, segurança, análise e colaboração, proporcionando uma solução completa e integrada.

De seguida, as ferramentas selecionadas serão descritas de forma a destacar como cada uma aborda os desafios enfrentados pelo banco e as razões para a sua escolha.

8.1 Collibra Data Intelligence

Figura 10 - Collibra

A Collibra Data Intelligence [1] é uma ferramenta desenvolvida para ajudar as empresas a organizar e gerir os seus dados de forma eficiente. Com funcionalidades como a criação de glossários e a catalogação de dados, ela assegura que a informação seja bem estruturada, uniformizada e de fácil acesso. Além disso, a ferramenta facilita a monitorização da origem dos dados e a implementação de políticas para garantir a sua qualidade e uso responsável.

Para enfrentar os desafios de inconsistência e baixa qualidade dos dados, o Collibra Data Intelligence oferece funcionalidades que permitem organizar informações em glossários centralizados, uniformizar dados e implementar regras que garantem a sua fiabilidade. Dessa forma, a solução ajuda a alinhar as equipas no uso correto das informações, promovendo uma governança eficaz e atendendo às necessidades específicas do banco.

8.2 Talend

Figura 11 – Talend

O Talend [2] é uma plataforma que oferece ferramentas para integração de dados, permitindo combinar e sincronizar informações de múltiplas fontes para fornecer uma visão unificada. Foi selecionado para resolver os problemas de integração entre sistemas, como CRM e ERP. Ele facilita a conexão entre diferentes sistemas e garante que os dados sejam transferidos de forma correta e segura. Além disso, oferece funcionalidades de monitorização e validação em tempo real, eliminando silos de dados e promovendo fluxos consistentes e eficientes.

8.3 Microsoft Power BI

Figura 12 - Microsoft Power BI

O Microsoft Power BI [3] é uma ferramenta de análise e visualização de dados que transforma informações complexas em relatórios e *dashboards* interativos. A solução permite criar visualizações claras e intuitivas, que ajudam os gestores a acompanhar indicadores-chave de desempenho (KPIs) e identificar tendências. Para o banco, o Power BI é uma boa opção para suportar a criação de relatórios interativos com base nos dados já integrados e organizados pelo Talend e Collibra. A ferramenta é essencial para apoiar decisões estratégicas, fornecendo dados atualizados e apresentados de forma acessível.

8.4 Microsoft SharePoint

Figura 13 - Microsoft SharePoint

O Microsoft SharePoint [4] é uma plataforma de colaboração e gestão documental que facilita o armazenamento, organização e partilha de informações importantes. A ferramenta permite criar bibliotecas centralizadas para documentos, configurar permissões de acesso para diferentes equipas e automatizar fluxos de aprovação. No banco, o SharePoint foi escolhido para apoiar a gestão de políticas, relatórios e documentos importantes, em que promove o trabalho colaborativo e garante que as equipas tenham acesso seguro e organizado às informações necessárias.

8.5 Implementação

A implementação das ferramentas será feita seguindo as fases do *roadmap* do Programa de Governança e Segurança de Dados. Cada ferramenta será configurada e usada em momentos específicos, tendo em conta as dependências entre as etapas e os prazos definidos. O objetivo é garantir que todas as soluções sejam aplicadas de forma organizada, resolvendo os problemas identificados de maneira eficiente.

A Tabela 21 mostra como cada ferramenta será utilizada na prática, alinhando as suas funcionalidades às fases do *roadmap*. Ela explica as ações necessárias para implementar cada solução e como estas contribuem para alcançar os objetivos do programa.

Tabela 21 - Funcionalidades das Ferramentas

Problemas Enfrentados	Ferramenta	Como Aplicar na Ferramenta	Fase do Roadmap
Inconsistências e má qualidade dos dados	Collibra Data Intelligence	1. Configurar o módulo de Data Catalog para identificar e catalogar todos os dados importantes do banco e organização de metadados; 2. Criar glossários para definir e uniformizar termos usados nas bases de dados; 3. Implementar regras de validação e workflows para revisão e aprovação de dados críticos; 4. Monitorizar periodicamente os dados para identificar e corrigir problemas de qualidade.	Criação do catálogo de dados e implementação de *Data Stewardship*.

Integração dos sistemas de CRM e ERP	Talend Data Fabric	1. Configurar fluxos de ETL para integrar dados do CRM e ERP; 2. Criar regras de transformação de campos (ex.: normalizar nomes, formatos de datas); 3. Implementar processos para identificar duplicados e consolidar informações de clientes; 4. Ativar a monitorização em tempo real para verificar possíveis erros durante os fluxos de integração.	Integração de dados e criação da visão única dos clientes.
Relatórios e suporte à decisão	Microsoft Power BI	1. Usar os dados integrados pelo Talend e organizados pelo Collibra; 2. Criar *dashboards* com visualizações de KPIs definidos pelas equipas de negócio. 3. Automatizar a atualização dos relatórios com base nos dados recebidos em tempo real; 4. Configurar permissões para que gestores e equipas acedam apenas aos relatórios relevantes para as suas áreas.	Criação de relatórios executivos e *dashboards* baseados em KPIs.
Gestão documental e colaboração	Microsoft SharePoint	1. Criar bibliotecas organizadas para guardar documentos (relatórios, políticas, manuais); 2. Configurar níveis de acesso e permissões para cada equipa (ex.: RH, TI, Finanças); 3. Fornecer formação para as equipas utilizarem as funcionalidades de partilha e edição colaborativa em tempo real.	Desenvolvimento de políticas e gestão colaborativa.

Conclusão

O presente relatório destacou a importância da implementação de um Programa de Governança e Segurança de Dados (PGSD) no Banco InovaData, com vista à maximização do valor estratégico dos dados, à melhoria da eficiência operacional e ao alinhamento às exigências regulatórias. O projeto demonstrou que a governança de dados não é apenas uma ferramenta para resolver problemas internos, mas um pilar essencial para sustentar a competitividade da organização num mercado cada vez mais digital e orientado por dados.

Através de uma abordagem estruturada, foram identificadas iniciativas estratégicas, definidas metas claras, e atribuídas responsabilidades específicas, com foco na clareza e eficácia na implementação do programa. A integração de ferramentas tecnológicas avançadas, aliada a práticas consistentes de gestão de dados e formação dos colaboradores, foi fundamental para alcançar os objetivos delineados.

Adicionalmente, a estrutura operacional proposta, incluindo a Matriz RACI e os diferentes papéis atribuídos aos *stakeholders*, permite estabelecer uma governança robusta e sustentável. A gestão de metadados e a criação de um glossário e dicionário de dados constituíram um alicerce essencial para assegurar a consistência e a compreensão dos dados em toda a organização, onde se alinham as práticas a normas reconhecidas internacionalmente.

Por fim, este relatório enfatizou que o sucesso do programa dependerá da adesão contínua de todas as partes interessadas, da monitorização regular dos progressos e da capacidade de adaptação às novas necessidades e desafios do mercado. O Banco InovaData, com este projeto, posiciona-se como uma organização *data-driven*, preparada para inovar, crescer de forma sustentável e garantir a confiança dos seus clientes e *stakeholders*.

Referências

[1] COLLIBRA. *Collibra Platform - AI Governance*. Disponível em: https://www.collibra.com/us/en/products/collibra-platform#tabs-productTabs-ai-governance. Acesso em: 15 jan. 2025.

[2] TALEND. *Talend Data Fabric*. Disponível em: https://www.talend.com/products/data-fabric/. Acesso em: 15 jan. 2025.

[3] MICROSOFT. *Microsoft Power BI*. Disponível em: https://www.microsoft.com/pt-pt/power-platform/products/power-bi?market=pt. Acesso em: 15 jan. 2025.

[4] MICROSOFT. *Microsoft SharePoint Collaboration*. Disponível em: https://www.microsoft.com/pt-pt/microsoft-365/sharepoint/collaboration. Acesso em: 15 jan. 2025.

[5] WORLD BANK. Glossary: A Dictionary of Terms Used in Project Preparation and Implementation. Disponível em: https://documents1.worldbank.org/curated/ar/541831468326979631/pdf/322800PUB00PUB0d0bank0glossary01996.pdf. Acesso em: 1 jan. 2025.

Bibliografia

LADLEY, John. *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program*. 2. ed. Academic Press, 2020.

DAMA INTERNATIONAL. *DAMA-DMBOK: Data Management Body of Knowledge*. 2. ed. Technics Publications, 2017.

Data Governance Committee Charter Template. Disponível em: https://myipleiria-my.sharepoint.com/:w:/g/personal/nuno_salvador_ipleiria_pt/ERMoccj-BEtJi-NO8BrdVtEBgJk7cILLA5jfZZ_4qxVH5A?rtime=VzXHX9w73Ug. Acesso em: 23 nov. 2024.

Netgrafia

Astera. Gestão de Metadados. Disponível em: https://www.astera.com/pt/type/blog/metadata-management/. Acesso em: 17 dez. 2024.

Ishikawa, M. Qual é a diferença entre catálogo de dados, glossário de negócios e dicionário de dados?. Medium. Disponível em: https://medium.com/%40imishikawa/qual-%C3%A9-a-diferen%C3%A7a-entre-cat%C3%A1logo-de-dados-gloss%C3%A1rio-de-neg%C3%B3cios-e-dicion%C3%A1rio-de-dados-5cd66fbc9c1b. Acesso em: 17 dez. 2024.

ABRACD. Glossário de Dados ou Dicionário de Dados. Disponível em: https://abracd.org/2020/10/19/glossario-de-dados-ou-dicionario-de-dados. Acesso em: 17 dez. 2024.

Data Geeks. Glossário dos Dados. Disponível em: https://www.datageeks.com.br/glossario-dos-dados/. Acesso em: 17 dez. 2024.

UC Merced Library. Data Dictionaries. Disponível em: https://library.ucmerced.edu/data-dictionaries. Acesso em: 19 dez. 2024.

Splunk. Data Dictionary. Disponível em: https://www.splunk.com/en_us/blog/learn/data-dictionary.html. Acesso em: 19 dez. 2024.

Dataversity. What is a Data Dictionary?. Disponível em: https://www.dataversity.net/what-is-a-data-dictionary/. Acesso em: 19 dez. 2024.

World Bank. Glossary: A Dictionary of Terms Used in Project Preparation and Implementation. Disponível em: https://documents1.worldbank.org/curated/ar/541831468326979631/pdf/322800PUB00PUB0d0bank0glossary01996.pdf. Acesso em: 7 jan. 2025.

DataCamp. What is Metadata?. Disponível em: https://www.datacamp.com/pt/blog/what-is-metadata. Acesso em: 7 jan. 2025.

SaferNet. O que são os metadados?. Disponível em: https://new.safernet.org.br/content/o-que-s%C3%A3o-os-metadados. Acesso em: 7 jan. 2025.

DP6. Gerenciamento de metadados e governança de dados: desvendando a estratégia oculta para o sucesso. Disponível em: https://blog.dp6.com.br/gerenciamento-de-metadados-e-governan%C3%A7a-de-dados-desvendando-a-estrat%C3%A9gia-oculta-para-o-sucesso-69a3fa916401. Acesso em: 17 jan. 2025.

Castor. The Role of Metadata in Data Governance. Disponível em: https://www.castordoc.com/blog/the-role-of-metadata-in-data-governance. Acesso em: 17 jan. 2025.

UK Government. Meet the Data Quality Dimensions. Disponível em: https://www.gov.uk/government/news/meet-the-data-quality-dimensions. Acesso em: 17 jan. 2025.

WIKIPEDIA. *Collibra*. Disponível em: https://nl.wikipedia.org/wiki/Collibra. Acesso em: 19 jan. 2025.

WIKIPEDIA. *Talend*. Disponível em: https://en.wikipedia.org/wiki/Talend. Acesso em: 19 jan. 2025.

WIKIPEDIA. *Microsoft Power BI*. Disponível em: https://en.wikipedia.org/wiki/Microsoft_Power_BI. Acesso em: 19 jan. 2025.

WIKIPEDIA. *SharePoint*. Disponível em: https://en.wikipedia.org/wiki/SharePoint. Acesso em: 19 jan. 2025.

Anexos

Anexo I - Estatuto do Comité de Governança de Dados - Banco InovaData

Comité de Governança de Dados

Artigo I. Autoridade

(a) Este estatuto autoriza formalmente o Comité de Governança de Dados (CGD), Comité Executive, do Banco InovaData a operar como a autoridade central para a governança de dados dentro da organização. O CGD está autorizado a estabelecer políticas, padrões e práticas para garantir a gestão e a utilização adequados dos ativos de dados.

Artigo II. Missão

(a) A missão do Comité de Governança de Dados é aumentar o valor, a qualidade, a segurança e a conformidade dos ativos de dados do banco, implementando uma estrutura sólida de governança. Esta estrutura estará alinhada aos requisitos regulatórios e aos objetivos estratégicos do negócio.

Artigo III. Metas e Objetivos Primários

(a) As metas do Comité de Governança de Dados são:

1. Garantir a precisão, consistência e segurança dos dados em todas as unidades de negócio.
2. Promover a tomada de decisões baseada em dados em todos o
3. s níveis organizacionais.
4. Alcançar conformidade com todos os frameworks regulatórios relevantes, incluindo o RGPD.

(b) Os objetivos primários do Comité de Governança de Dados são:

1. Desenvolver e aplicar políticas e procedimentos de governança de dados.
2. Monitorizar e criar métricas de qualidade e conformidade de dados.
3. Facilitar a colaboração interdepartamental para otimizar as práticas de gestão de dados.

Artigo IV. Composição e Qualificação de Serviço

(a) O Comité de Governança de Dados será composto por 5 membros permanentes com direito a voto:

1. Diretor de Sistemas de Informação (CIO) - Presidente.
2. Diretor de Gestão de Riscos (CRO) - Vice-presidente.
3. Diretor de Finanças (CFO).
4. Diretora de Marketing (CMO).
5. Diretor de Compliance e Conformidade Regulatória.

(b) Especialistas no assunto, convidados e apresentadores podem ser convidados a participar conforme necessário.

(c) O Presidente e o Vice-presidente são nomeados pelo conselho executivo e terão mandato de 2 anos.

(d) Substitutos são permitidos para participar em reuniões e votar em nome dos membros permanentes na sua ausência.

Artigo V. Votação

(a) As votações e decisões serão conduzidas utilizando o modelo de maioria. Um mínimo de 60% dos membros votantes deve estar presente para constituir quórum.

(b) Na ausência de quórum, o Presidente pode realizar uma reunião informativa ou adiar a sessão.

Artigo VI. Reuniões

(a) O Comité de Governança de Dados irá reunir-se trimestralmente, com reuniões adicionais agendadas conforme necessário.

(b) As reuniões podem ser realizadas virtualmente ou na sede do Banco InovaData.

Artigo VII. Papéis e Responsabilidades

(a) **Responsabilidades do Presidente:**

1. Agendar e supervisionar as reuniões do CGD.
2. Aprovar agendas de reuniões e listas de participantes.
3. Garantir que a documentação, como atas e relatórios, seja preparada e distribuída.
4. Relatar o status das metas e objetivos de governança de dados.

(b) **Responsabilidades do Vice-presidente:**

1. Assumir as responsabilidades do Presidente na sua ausência.

(c) **Responsabilidades dos Membros Votantes:**

1. Participar de todas as reuniões presencialmente ou por meio de substituto.
2. Rever e fornecer contribuições sobre políticas e iniciativas.
3. Apoiar a implementação das práticas de governança de dados aprovadas nas suas respectivas unidades.

(d) **Papéis Operacionais:**

1. **Data Stewards:** Gerir a qualidade dos dados e aplicar práticas de governança.
2. **Data Custodians:** Garantir o acesso seguro e eficiente dos ativos de dados.
3. **Diretor de Conformidade:** Monitorizar a adesão às regulamentações e realizar auditorias regulares.

Artigo VIII. Relatórios de Status

(a) O Presidente preparará um relatório de status para revisão pelos membros do comité pelo menos 2 semanas antes de cada reunião agendada.

(b) O relatório incluirá:

1. Atualizações sobre o progresso das metas de governança de dados.
2. Barreiras identificadas e resoluções propostas.
3. Recomendações para melhorar os processos de governança de dados.

Artigo IX. Aprovação do Estatuto

(a) Este estatuto é aprovado pelo Comité de Governança de Dados em [Inserir Data de Aprovação].

(b) Os membros abaixo assinados reconhecem sua revisão e aprovação deste estatuto.

Assinaturas:

NOME:_____
CARGO:_____
DATA: _____

Anexo II – Diagrama de *Gantt* – *Roadmap* PGSD

Legenda:

- Prioridade Alta
- Prioridade Média
- Prioridade Baixa

Anexo III – Política de Metadados

Objetivo

O objetivo desta política é estabelecer orientações para a criação, gestão e divulgação de metadados associados a conjuntos de dados publicados pelo Banco InovaData. Esta política tem por objetivo garantir a qualidade, a coerência e a interoperabilidade dos dados, facilitando a sua descoberta, acessibilidade e reutilização.

Âmbito

Esta política aplica-se a todos os conjuntos de dados criados, recolhidos ou mantidos pelo Banco InovaData.

Definições

Termo	Definição
Metadados	Informação estruturada que descreve, explica, localiza ou facilita a recuperação, utilização ou gestão de um recurso de informação.
Normas de Metadados	Diretrizes e especificações para a criação, gestão e manutenção de metadados
Repositório de metadados	Uma localização central onde os metadados são armazenados e geridos.
Conjunto de dados	Um conjunto de elementos de dados relacionados, organizados num formato estruturado.
Data Steward	Uma pessoa responsável pela gestão de um conjunto de dados e por garantir a sua qualidade e a exatidão dos metadados.
NIEM Core	Um quadro concebido para facilitar o intercâmbio de informações entre diferentes domínios, como a justiça, a segurança pública, a gestão de emergências e a saúde, que faz parte do Modelo Nacional de Intercâmbio de Informações (NIEM).

Política

Todos os funcionários do Banco InovaData devem aderir às normas de metadados estabelecidas quando criam, gerem ou utilizam metadados.

Normas de Metadados

Todos os metadados devem estar em conformidade com as seguintes normas:

- NIEM Core: Um conjunto normalizado de componentes de dados que pode ser utilizado em vários domínios para garantir a interoperabilidade e o intercâmbio coerente de informações.
- Norma de Metadados *Federal Geographic Data Committee* (FGDC): Uma norma para metadados geoespaciais.

Modelo de Metadados

- O modelo de metadados do Banco InovaData define o conjunto mínimo de metadados que devem acompanhar todos os dados criados ou adquiridos pelo banco. Para fornecer um quadro para a gestão de metadados no Portal de Dados Abertos, foram definidas categorias e todos os metadados serão categorizados de acordo com estas categorias.

- Todos os sistemas de informação da Agência devem incluir os seguintes elementos de dados em cada uma das seguintes categorias.

Elemento	Descrição	Exemplo
Título	Um nome descritivo do conjunto de dados	Sistema Core Banking
Descrição	Um resumo do conjunto de dados, incluindo o seu objetivo e conteúdo	Operações diárias, desde a abertura de contas, processamento de depósitos e levantamentos, até à gestão de empréstimos
Agência	A entidade responsável pela publicação do serviço ou recurso.	VDH, VEC, USDA
Data	A data em que o conjunto de dados foi criado ou publicado	01/01/2022
Classificação		Nível 0-3; Altamente confidencial
Categoria	Palavras-chave ou frases que descrevem o conteúdo do conjunto de dados	Económico, ambiental, segurança pública
Frequência de atualização	Ciclo de renovação ou atualização planeado	Anualmente, mensalmente, diariamente, de hora a hora, ad hoc
Formato	O formato do ficheiro do conjunto de dados	CSV, JSON, XML
Opcional		
Fonte	Informação sobre a origem do conjunto de dados.	Sistema Core Banking
Identificador	Um identificador único para o conjunto de dados	COVODGA1000A
Direitos	Informações sobre os direitos detidos no e sobre o conjunto de dados, incluindo o licenciamento	Domínio público, apenas COV

Criação e manutenção de metadados

- Os metadados devem ser criados ao mesmo tempo que o conjunto de dados e atualizados sempre que o conjunto de dados for modificado.
- As informações confidenciais ou sensíveis não devem ser incluídas nos metadados sem a devida autorização.
- Devem ser utilizados processos de gestão das alterações e de controlo das versões para garantir uma auditoria e uma gestão adequadas.
- Os registos de metadados devem ser revistos anualmente pelos administradores de dados para garantir que continuam a ser exatos e relevantes.

Os metadados serão conservados para os dados que tenham sido apagados, incluindo a data de apagamento, durante um período de dois anos após a data de apagamento.

Garantia de qualidade

- Os proprietários dos dados, em conjunto com o seu responsável designado, devem monitorizar e verificar a qualidade dos metadados do sistema para garantir a sua exatidão, coerência e fiabilidade.
- Os metadados devem ser revistos por uma segunda parte para garantir a sua exatidão e integridade antes da publicação.
- Podem ser utilizadas ferramentas automatizadas para verificar a conformidade com as normas de metadados e identificar erros.

Publicação e acessibilidade

- Deve ser criado um repositório de metadados, ou a agência pode utilizar o repositório centralizado de metadados da ODGA, para armazenar e gerir metadados.
- Os metadados devem estar num formato legível por máquina para facilitar a descoberta e a reutilização dos dados.
- Os proprietários de dados, em conjunto com os seus administradores de dados designados, devem implementar e manter medidas de segurança adequadas para os metadados do sistema, incluindo a definição de permissões de acesso e a garantia de cifragem, conforme necessário.
- Recomenda-se que os metadados sejam disponibilizados a todos os funcionários da Commonwealth of Virginia, exceto se for especificamente solicitado que os metadados de um conjunto de dados sejam restringidos.

Conformidade e aplicação da lei

- O cumprimento desta política é obrigatório para todos os departamentos e indivíduos envolvidos na gestão de conjuntos de dados.
- O incumprimento pode dar origem a medidas corretivas determinadas pela direção do Banco InovaData.

Formação e apoio

- A equipa de governação de dados do e o Gabinete de Governação e Análise de Dados (ODGA) proporcionarão sessões de formação sobre normas de metadados, como o NIEM Core e as melhores práticas, a todos os administradores de dados e pessoal relevante
- O apoio e os recursos contínuos estarão disponíveis através do Data Steward do Banco InovaData e do Gabinete de Governação e Análise de Dados (ODGA).

Revisão da política

Esta política será revista e atualizada anualmente a partir da data de aprovação, ou mais frequentemente, se necessário. Os membros do pessoal que desejem fazer comentários sobre a política podem enviar as suas sugestões.

Anexo IV – Dicionário de Dados

Sistema Core Banking

Clientes					
Nome do Campo	ID_cliente	Nome_cliente	Numero_identificacao	Endereco	Informacoes_contato
Descrição	Identificador único do cliente.	Nome completo do cliente.	Número de identificação do cliente (exemplo: número de cartão de cidadão, CPF).	Endereço completo do cliente.	Informações de contato do cliente (telefone, email, etc.).
Tipo de Dados	VARCHAR	VARCHAR	INTEGER	VARCHAR	VARCHAR
Tamanho	-	255	20	500	255
Formato	"C" seguido de número sequencial (ex: "C1", "C2", "C3", ...)	-			
Valor padrão	Criado de forma automática	-			
Valores Permitidos	-				
Restrições	Chave primária, único	Obrigatório	Único, obrigatório	Obrigatório	Obrigatório
Exemplo de Valor	C1, C2, C3, C4	João Silva	123456789	Rua Principal, 1	joao@email.com, 123-456-789
Notas Adicionais	Utilizado para distinguir clientes no sistema.	-	Pode ser o número do cartão de identificação nacional, NIF ou outro dado identificador único legalmente válido.	Inclui rua, número, cidade, código postal.	Pode incluir múltiplos meios de contato separados por vírgula.

Contas					
Nome do Campo	Numero_conta	ID_cliente	Saldo_conta	Tipo_conta	Data_abertura
Descrição	Número único da conta bancária.	Identificador do cliente associado à conta.	Valor disponível na conta.	Tipo da conta (exemplo: Corrente, Poupança, etc.).	Data em que a conta foi aberta.
Tipo de Dados	INTEGER	VARCHAR	DECIMAL	VARCHAR	DATE
Tamanho	20	-	-	20	-
Formato	Numérico	-			"AAAA/MM/DD"

Valor padrão	Criado de forma automática	-	0.00	-	Criado de forma automática
Valores Permitidos	-				
Restrições	Único, obrigatório	Referência para a tabela de Clientes	-	Obrigatório	Obrigatório
Exemplo de Valor	1001	C1	5000.00	Poupança	2023-01-15
Notas Adicionais	O número da conta deve ser único para cada cliente e conta.	O ID do cliente refere-se ao campo "ID_cliente" da tabela "Clientes".	-	Define o tipo de conta do cliente.	-

Transações						
Nome do Campo	ID_transacao	Numero_conta_origem	Numero_conta_destino	Valor_transacao	Data_hora_transacao	Tipo_transacao
Descrição	Identificador único da transação.	Número da conta de origem da transação.	Número da conta de destino da transação.	Valor monetário da transação.	Data e hora exatas em que a transação foi realizada.	Tipo da transação (exemplo: "Depósito", "Transferência", "Saque").
Tipo de Dados	INTEGER	VARCHAR	VARCHAR	DECIMAL	DATETIME	VARCHAR
Tamanho	-	20	20	-	-	20
Formato	-	-	-	-	-	-
Valor padrão	-					
Valores Permitidos	Único e numérico	Número de conta válido	Número de conta válido	Valores numéricos positivos	Qualquer data e hora válidas	"Transferência", "Saque", "Depósito", etc.
Restrições	Chave primária, único	Referência para a tabela de **Contas**	Referência para a tabela de **Contas**	Deve ser maior ou igual a 0.00	Obrigatório	Obrigatório
Exemplo de Valor	2001	1001	1002	500.75	20/01/2025 14:30:00	Transferência
Notas Adicionais	O ID da transação é único para cada operação.	-	-	-	Criado de forma automática	Define o tipo de transação realizada.

Empréstimos						
Nome do Campo	ID_emprestimo	ID_cliente	Valor_emprestimo	Taxa_juros	Prazo_emprestimo	Status_emprestimo
Descrição	Identificador único do empréstimo.	Identificador único do cliente associado ao empréstimo.	Valor total do empréstimo.	Taxa de juros anual aplicada ao empréstimo.	Prazo do empréstimo em meses.	Status atual do empréstimo (exemplo: "Aprovado", "Em andamento", "Pago").
Tipo de Dados	INTEGER	VARCHAR	DECIMAL	DECIMAL	INTEGER	VARCHAR
Tamanho	-	-	-	-	-	20
Formato	Numérico	"C1", "C2", "C3", ... (ID do cliente)	Ex: 10000.00 (formato monetário)	Ex: 5.00 (percentual de taxa de juros)	Ex: 36 (meses)	"Aprovado", "Em andamento", "Pago", etc.
Valor padrão	Gerado automáticamente	-	-	-	-	"Em andamento"
Valores Permitidos	Único, numérico	ID de cliente válido (como "C1", "C2", ...)	Valores numéricos positivos	Taxas de juros positivas	Prazo em meses (ex: 12, 24, 36, ...)	"Aprovado", "Em andamento", "Pago"
Restrições	Chave primária, único	Referência para a tabela Clientes	Deve ser maior que 0.00	Deve ser 0.00 ou maior	Deve ser maior que 0 (meses)	Obrigatório
Exemplo de Valor	3001	C1	10000.00	5.0	24 meses	Ativo
Notas Adicionais	O ID do empréstimo é único para cada empréstimo concedido.	-	-	Taxa de juros anual que será aplicada ao empréstimo.	O prazo do empréstimo é o número de meses até o pagamento total.	Status deve refletir o estado atual do empréstimo.

Funcionários					
Nome do Campo	ID_funcionario	Nome_funcionario	Cargo	Departamento	Informacoes_contato
Descrição	Identificador único do funcionário.	Nome completo do funcionário.	Cargo ou função ocupada pelo funcionário.	Departamento ou área onde o funcionário trabalha.	Informações de contato do funcionário (telefone, email, etc.).
Tipo de Dados	INTEGER	VARCHAR	VARCHAR	VARCHAR	VARCHAR
Tamanho	-	255	100	100	255
Formato	-				
Valor padrão	Gerado automáticamente	-			

Valores Permitidos	Único, numérico	-	-	Qualquer departamento válido	Informações de contacto separadas por vírgulas
Restrições	Chave primária, único	Obrigatório	Obrigatório	Obrigatório	Obrigatório
Exemplo de Valor	5001	Jose Afonso	Gerente	Filial	ana@email.com, 555-123-789
Notas Adicionais	O ID do funcionário é único para cada pessoa.	O nome completo do funcionário é exigido.	O cargo define a posição do funcionário dentro da organização	O departamento define a área de atuação do funcionário.	Pode incluir múltiplos meios de contato separados por vírgula.

Registos de acesso					
Nome do Campo	ID_registo	ID_funcionario	Data_hora_acesso	Tipo_acesso	Endereco_IP
Descrição	Identificador único do registo de acesso.	Identificador único do funcionário que fez o acesso.	Data e hora exatas do acesso ao sistema.	Tipo de acesso realizado (exemplo: "Login", "Logout").	Endereço IP de onde o acesso foi feito.
Tipo de Dados	INTEGER	VARCHAR	DATETIME	VARCHAR	VARCHAR
Tamanho	-	-	-	20	15
Formato	-	-	-	Ex: "Login", "Logout", “Acesso a dados sensíveis”, etc...	Endereço IPV4 no formato padrão (ex: "192.168.1.1")
Valor padrão	Gerado automaticamente - Gerado automaticamente	-			
Valores Permitidos	Único, numérico	ID de funcionário válido (como "C1", "C2", ...)	Qualquer data e hora válidas	"Login", "Logout", etc..	Endereço IP válido
Restrições	Chave primária, único	Referência para a tabela Funcionários	Obrigatório	Obrigatório	Obrigatório
Exemplo de Valor	7001	5001	2023-04-05 08:30:00	Login	192.168.1.107
Notas Adicionais	O ID do registo é único para cada acesso.	O ID do funcionário refere-se à tabela Funcionário.	A data e hora devem refletir o momento exato do acesso.	Pode ser "Login", "Logout", ou outros tipos específicos pré-definidos.	O endereço IP é registado para fins de auditoria e segurança.

Sistema de CRM

Clientes					
Nome do Campo	ID_cliente	Nome	Email	Telefone	Endereco
Descrição	Identificador único do cliente.	Nome completo do cliente.	Endereço de email do cliente.	Número de telefone do cliente.	Endereço completo do cliente.
Tipo de Dados	VARCHAR	VARCHAR	VARCHAR	VARCHAR	VARCHAR
Tamanho	-	255	255	20	500
Formato	-	-	Ex: "nome@dominio.com"	Ex: "123-456-7890 "	Inclui rua, número, cidade, distrito, etc.
Valor padrão	-				
Valores Permitidos	Único, numérico	-	Formato válido de email	Formato válido de telefone (numérico)	Qualquer endereço válido
Restrições	Chave primária, único	Obrigatório	Único, obrigatório	-	-
Exemplo de Valor	C2	João Silva	joao@email.com	123-456-7890	Rua A, nº 123
Notas Adicionais	O ID do cliente é único para cada cliente registado.	O nome completo é exigido.	O email deve ser único e válido.	O telefone pode incluir o código de área e o número de celular.	O endereço inclui rua, número, cidade, estado, e, se aplicável, o código postal.

Contas Bancárias						
Nome do Campo			ID_conta	ID_cliente	Tipo_conta	Saldo_atual	Data_abertura
Descrição			Identificador único da conta bancária.	Identificador único do cliente associado à conta.	Tipo de conta (exemplo: "Corrente", "Poupança").	Valor atual do saldo da conta.	Data em que a conta foi aberta.
Tipo de Dados			INTEGER	VARCHAR	VARCHAR	DECIMAL	DATETIME
Tamanho			-	-	20	-	-
Formato			-	C1,C2,C3,...	Ex: "Corrente", "Poupança"....	Ex: 1500.75 (formato monetário)	“AAAA/MM/DD”
Valor padrão	-	0.00	-				
Valores Permitidos			Único, numérico	-	"Corrente", "Poupança", "Investimento", etc.	Qualquer valor numérico.	-
Restrições			Chave primária, único	Referência para a tabela Clientes	Obrigatório	-	Obrigatório
Exemplo de Valor			1001	C1	Poupança	5000.00	2023-01-15
Notas Adicionais			O ID da conta deve ser único	O ID do cliente refere-se ao	Define o tipo de conta bancária do cliente.	O saldo deve refletir o valor atual	A data deve seguir o

	para cada conta bancária.	campo ID_cliente na tabela Clientes.		disponível na conta.	formato definido.

Produtos Bancários				
Nome do Campo	ID_produto	Nome_produto	Descricao	Preco_mensal
Descrição	Identificador único do produto.	Nome do produto.	Descrição detalhada do produto.	Preço mensal do produto ou serviço.
Tipo de Dados	INTEGER	VARCHAR	VARCHAR	DECIMAL
Tamanho	-	255	500	20
Formato	-			
Valor padrão	-	-	-	0.00
Valores Permitidos	Único, numérico	-	-	Valores numéricos positivos ou negativos
Restrições	Chave primária, único	Obrigatório	-	-
Exemplo de Valor	2001	Conta Poupança	Conta de poupança com juros	5.00
Notas Adicionais	O ID do produto deve ser único.	Nome do produto deve ser único e descritivo.	-	-

Interações com Clientes					
Nome do Campo	ID_interacao	ID_cliente	Data_hora	Tipo_interacao	Descricao
Descrição	Identificador único da interação.	Identificador único do cliente associado à interação.	Data e hora exatas da interação.	Tipo de interação (exemplo: "Chamada", "Email", "Suporte").	Descrição detalhada da interação realizada com o cliente.
Tipo de Dados	INTEGER	VARCHAR	DATETIME	VARCHAR	VARCHAR
Tamanho	-	-	-	20	500
Formato	-	-	-	-	-
Valor padrão	-	-	-	-	-
Valores Permitidos	Numérico	ID de cliente válido	Qualquer data e hora válidas.	Qualquer tipo de interação válido	-
Restrições	Chave primária, único	Referência para a tabela Clientes	Obrigatório	Obrigatório	Obrigatório
Exemplo de Valor	3001	C1	2023-03-10 09:30:00	Chamada	Discussão de Conta
Notas Adicionais	O ID da interação deve ser único para cada evento registado.	O ID do cliente refere-se à tabela Clientes.	A data e hora devem refletir o momento exato da interação.	O tipo pode ser "Chamada", "Email", "Suporte", ou outros tipos de interação.	Descrição pode ser detalhada, incluindo o conteúdo ou objetivo da interação.

Notas				
Nome do Campo	ID_nota	ID_cliente	Conteudo	Data_criacao
Descrição	Identificador único da nota.	Identificador único do cliente associado à nota.	Texto completo da nota emitida.	Data de emissão da nota.
Tipo de Dados	INTEGER	VARCHAR	VARCHAR	DATE
Tamanho	-	-	500	-
Formato	-	-	Texto livre, descrevendo a nota	-
Valor padrão	Valor automático	-	-	-
Valores Permitidos	Único, numérico	ID de cliente válido (como "C1", "C2", ...)	Texto livre, sem formatação específica	Qualquer data válida
Restrições	Chave primária, único	Referência para a tabela Clientes	Obrigatório	Obrigatório
Exemplo de Valor	4001	C1	Cliente interessado em investimentos	2023-03-01
Notas Adicionais	O ID da nota deve ser único.	O ID do cliente refere-se à tabela Clientes.	A nota pode conter detalhes sobre interações ou transações.	A data deve seguir o formato " AAAA /MM/DD ".

Anexo V – Glossário de Dados

A

Análise de Dados: Uso de dados estruturados e não estruturados para gerar insights que suportem decisões estratégicas.

Análise de Risco: Avaliação de potenciais perdas financeiras associadas a empréstimos, investimentos ou outros fatores operacionais.

B

Big Data: Conjuntos massivos de dados gerados e processados pela organização para obter insights estratégicos.

Base de Dados Relacional: Estrutura de armazenamento de dados organizada em tabelas interconectadas por relações lógicas.

C

Core Banking: Sistema central que gerência operações bancárias diárias, como abertura de contas, processamento de depósitos e gestão de empréstimos.

CRM (Customer Relationship Management): Sistema utilizado para gerenciar relações com clientes, otimizando a experiência e personalizando os serviços oferecidos.

Compliance: Conformidade com regulamentações e leis aplicáveis, essencial para manter a credibilidade e operar no setor financeiro.

Cross-Selling: Estratégia de vendas que oferece produtos ou serviços adicionais aos clientes existentes, com base no histórico e comportamento.

Consolidação de Dados: Processo de reunir dados dispersos em diferentes sistemas para criar uma visão unificada e consistente.

Cargo: O título ou posição ocupada pelo funcionário dentro da organização, que descreve as suas responsabilidades e funções no ambiente de trabalho.

Conteúdo (Nota): O texto ou informações presentes na nota, que descrevem o motivo, observações ou detalhes relacionados à interação ou situação do cliente.

D

Data Center: Instalações em Faro e Braga que suportam a infraestrutura tecnológica do banco, com sistemas de replicação e planos de recuperação de desastres.

Dados Sensíveis: Informações protegidas por regulamentações, incluindo dados pessoais e financeiros, que exigem maior nível de segurança.

Data: A data do registo.

Data de Abertura: A data em que a conta foi criada ou aberta para o cliente, marcando o início das atividades dessa conta dentro do sistema da organização.

Data de Contratação: Data de contratação de colaborador.

Data e Hora da Transação: A data e a hora em que a transação foi realizada, essencial para registar e acompanhar o histórico de transações de forma temporal.

Data e Hora do Acesso: A data e a hora exatas em que o acesso ao sistema foi realizado, essencial para monitoramento e auditoria de atividades dos funcionários.

Data e Hora: A data e hora exatas em que a interação ocorreu.

Data de Criação: A data e hora em que registo foi criado ou registado no sistema, ajudando a contextualizar o momento em que a informação foi inserida.

Data de Emissão: A data em que o cartão foi emitido ou disponibilizado para o cliente, marcando o início da validade do cartão.

Data de Expiração: A data até a qual o cartão é válido, após a qual o cliente precisará renovar ou solicitar um novo cartão.

Data do Pedido: A data em que o pedido foi realizado, essencial para o registo temporal e para acompanhar o processo de pedidos ao longo do tempo.

Departamento: A divisão ou área da organização à qual o funcionário pertence, como, por exemplo, Recursos Humanos, Marketing, Vendas, etc., indicando o setor em que exerce as suas atividades.

Descrição (produto): Texto explicativo sobre as características e funcionalidades do produto, detalhando o que ele oferece, seus benefícios e usos, para ajudar na compreensão e venda do produto.

Descrição (Interação): Detalhes sobre a interação, incluindo o conteúdo discutido, ações tomadas, problemas resolvidos ou solicitações feitas durante o contato entre o cliente e a organização.

Descrição (Despesas): Detalhe ou explicação sobre a despesa, indicando o motivo ou natureza da despesa, como, por exemplo, "pagamento de fornecedores", "despesas de viagem", etc.

E

ERP (Enterprise Resource Planning): Sistema integrado para gerenciar recursos, finanças, operações e recursos humanos, promovendo eficiência e conformidade regulatória.

ExpressVPN: Tecnologia de rede virtual privada usada para conexões seguras entre filiais, balcões e a sede do banco.

Endereço: O local onde o cliente reside ou onde a correspondência deve ser enviada. Inclui elementos como rua, número, cidade, código postal e país.

Endereço IP: O endereço de protocolo de internet (IP) associado ao dispositivo utilizado pelo funcionário para aceder ao sistema, fornecendo informações sobre a localização e a origem do acesso.

Email: Endereço de correio eletrônico do indivíduo ou entidade, utilizado para comunicação digital. Pode ser utilizado para correspondência, notificações ou marketing, dependendo do contexto.

Estado do Cartão: A situação atual do cartão, como "Ativo", "Suspenso", "Cancelado", "Vencido", etc., indicando a validade e a possibilidade de uso do cartão.

Estado do Pedido: A situação atual do pedido, como "Pendente", "Em Processamento", "Concluído", "Cancelado", entre outros, indicando o progresso ou a conclusão do pedido no sistema.

F

Framework DAMA-DMBOK: Referencial para boas práticas na governança e gestão de dados.

Fraudes Bancárias: Atividades ilegais envolvendo manipulação de dados financeiros ou transações para obter vantagens indevidas.

G

Governança de Dados: Conjunto de políticas e práticas para gerenciar a qualidade, segurança e utilização de dados dentro da organização.

Gestão de Ativos e Passivos: Atividade financeira que envolve equilibrar receitas e despesas do banco para otimizar a liquidez e minimizar riscos.

Gestão de Liquidez: Garantia de que o banco possui recursos disponíveis para cumprir as suas obrigações financeiras diárias.

H

I

Interoperabilidade de Sistemas: Capacidade de diferentes sistemas (CRM, ERP, Core Banking) trocarem dados entre si de maneira eficiente.

ID do Cliente: Identificador único atribuído a cada cliente dentro do sistema da organização. Usado para distinguir e fazer referência a cada cliente de forma inequívoca.

ID da Transação: Identificador único atribuído a cada transação financeira realizada, utilizado para monitorizar e fazer referência a transações específicas no sistema.

ID do Empréstimo: Identificador único atribuído a cada empréstimo, utilizado para monitorizar e fazer referência a um empréstimo específico no sistema.

ID do Funcionário: Identificador único atribuído a cada funcionário da organização, utilizado para monitorizar e fazer referência ao funcionário no sistema.

ID do Registo: Identificador único atribuído a cada registo de acesso no sistema, utilizado para monitorizar e fazer referência a eventos específicos de acesso dos funcionários.

ID da Conta: Identificador único atribuído a cada conta dentro da organização, utilizado para monitorizar e fazer referência a uma conta específica no sistema.

ID do Produto: Identificador único atribuído a cada produto dentro do sistema da organização, utilizado para monitorizar e fazer referência a um produto específico.

ID da Interação: Identificador único atribuído a cada interação entre o cliente e a organização, utilizado para monitorizar e fazer referência a uma interação específica no sistema.

ID da Nota: identificador único atribuído a cada nota ou comentário gerado no sistema, utilizado para monitorizar e fazer referência a uma nota específica.

ID do Departamento (BU): Identificador único atribuído a cada departamento ou unidade de negócio (Business Unit - BU) dentro da organização, utilizado para monitorizar e fazer referência a um departamento específico no sistema.

ID da Despesa: Identificador único atribuído a cada despesa registada no sistema, utilizado para monitorizar e fazer referência a uma despesa específica.

Data e Hora: Identificador único atribuído a cada cartão no sistema, utilizado para monitorizar e fazer referência a um cartão específico.

ID do Item: Identificador único atribuído a cada item no sistema, utilizado para monitorizar e fazer referência a um item específico.

ID do Bloqueio: Identificador único atribuído a cada bloqueio de cartão, utilizado para monitorizar e fazer referência a um bloqueio específico no sistema.

ID do Pedido: Identificador único atribuído a cada pedido realizado, utilizado para monitorizar e fazer referência a um pedido específico no sistema.

Informações de Contato: Dados que permitem à organização entrar em contato com o cliente ou colaborador, como número de telefone, endereço de e-mail e outras formas de comunicação.

J

K

L

Limite de Crédito: O valor máximo que o cliente pode gastar utilizando o cartão de crédito, definido pela instituição financeira com base no perfil de crédito do cliente.

M

Monitorização de Risco: Acompanhamento contínuo de exposições a riscos financeiros e operacionais.

Montante: Valor total associado a uma transação, conta, pagamento ou qualquer outro processo financeiro. O montante pode referir-se a um valor em dinheiro, seja positivo (quantia a receber) ou negativo (quantia a pagar), dependendo do contexto.

Motivo: A razão pela qual o cartão foi bloqueado, como "Perda", "Suspeita de Fraude", "Excesso de Tentativas de Senha", entre outros, explicando a causa do bloqueio no sistema.

N

Nome do Cliente: O nome completo do cliente conforme registado nos documentos oficiais ou na organização. Este campo representa a identidade pessoal do cliente.

Número de Identificação: Um número único que identifica legalmente o cliente, como o número de cartão de cidadão, ex.: NIF, dependendo da jurisdição e do tipo de cliente.

Número da Conta: Identificador único associado a uma conta bancária ou de cliente, utilizado para monitorizar e gerenciar as transações realizadas nessa conta.

Número da Conta de Origem: O número da conta de onde o valor é retirado durante uma transação, representando a conta do cliente que inicia a transação.

Número da Conta de Destino: O número da conta para a qual o valor é transferido durante uma transação, representando a conta do cliente que recebe o valor.

Número do Cartão: O número único que identifica o cartão, utilizado para realizar transações financeiras e associar o cartão ao cliente no sistema de pagamentos.

Nome do Funcionário: Nome completo do funcionário conforme registado nos documentos oficiais ou sistema da organização, usado para identificar o colaborador.

Nome do Produto: Nome dado ao produto, utilizado para identificar e diferenciar o produto dentro da organização e entre os clientes.

Nome do Departamento: O nome do departamento ou unidade de negócio, utilizado para identificar e diferenciar o departamento dentro da estrutura organizacional, como "Recursos Humanos", "Financeiro", "Marketing", entre outros.

Nome do Item: O nome dado ao item, utilizado para identificar e diferenciar o item dentro do inventário ou catálogo de produtos.

O

Onboarding de Clientes: Processo de abertura de contas e integração inicial de clientes aos serviços e produtos do banco.

P

Plano de Recuperação de Desastres: Estratégia para restaurar operações em caso de falhas ou desastres, garantindo continuidade de negócios.

Privacidade de Dados: Garantia de que os dados pessoais dos clientes são protegidos e utilizados apenas com consentimento.

Planeamento Financeiro: Atividade de projetar receitas e despesas para garantir a saúde financeira do banco.

Prazo do Empréstimo: O período de tempo acordado para a devolução do valor emprestado, que pode ser em meses ou anos, dependendo das condições acordadas no contrato.

Preço Mensal: O custo do produto em termos mensais, caso seja uma cobrança recorrente, como no caso de subscrições ou serviços pagos periodicamente.

Preço Unitário: O custo de uma única unidade do item, geralmente expresso em uma moeda específica, e utilizado para calcular o valor total de uma compra ou transação envolvendo o item.

Q

Qualidade de Dados: Garantia de que os dados são precisos, consistentes, atualizados e relevantes para o negócio.

Quantidade Disponível: A quantidade atual do item disponível em estoque ou para venda, indicando o número de unidades disponíveis para transação ou distribuição.

R

Regulamento Geral de Proteção de Dados (RGPD): Legislação europeia que estabelece diretrizes para proteção de dados pessoais e privacidade.

Relatórios de Conformidade: Documentação que demonstra o cumprimento das normas regulatórias e operacionais.

S

Silos de Dados: Fragmentação de informações entre diferentes sistemas ou departamentos, dificultando a integração e análise.

Shadow IT: Sistemas ou soluções tecnológicas desenvolvidas e utilizadas sem a aprovação do departamento de TI, criando potenciais riscos de segurança e inconsistências.

Sistema de Gestão de Cartões: Sistema para administração de cartões de débito e crédito, incluindo emissão, bloqueio e transações.

Sistema de Business Intelligence (BI): Ferramenta para análise de dados, geração de relatórios e obtenção de insights para decisões estratégicas.

Sistema de Segurança e Prevenção de Fraudes: Tecnologia utilizada para monitorar e prevenir atividades suspeitas e proteger dados do banco.

Sistema de Backup e Recuperação: Solução para preservar a integridade e segurança dos dados, minimizando riscos de perda.

SAN (Storage Area Network): Rede de armazenamento que utiliza tecnologia Fibre Channel (FC) para oferecer espaço de armazenamento aos servidores e máquinas virtuais.

Segurança de Dados: Medidas adotadas para proteger informações sensíveis contra acessos não autorizados e violações.

Score de Crédito: Métrica usada para avaliar a capacidade de crédito de um cliente, com base em seu histórico financeiro.

Simulação de Crédito: Cálculo realizado para prever as condições de um empréstimo, como taxa de juros, parcelas e prazo.

Gestão de Reclamações: Processo de registar, acompanhar e resolver queixas apresentadas pelos clientes.

Saldo da Conta / Saldo Atual: O valor atual disponível na conta do cliente, que pode ser positivo (saldo devedor) ou negativo (saldo credor), dependendo do tipo de conta e das transações realizadas.

Status do Empréstimo: O estado atual do empréstimo, indicando se está ativo, pago, em atraso, inadimplente, ou com qualquer outro status que defina a situação do empréstimo no sistema.

T

Transformação Data-Driven: Estratégia para tornar o banco orientado por dados, onde decisões operacionais e estratégicas são baseadas em insights analíticos.

Thin Client: Equipamento projetado exclusivamente para conexões remotas, com processamento centralizado nos servidores, aumentando a segurança.

Transformação Digital: Processo de adoção de tecnologias para modernizar operações bancárias e integrar dados digitais ao negócio.

Taxa de Esforço: Métrica utilizada na análise de risco de crédito, indicando a percentagem da renda de um cliente comprometida com dívidas.

Taxa de Juros: A taxa percentual aplicada ao valor do empréstimo, que define o custo adicional que o cliente pagará sobre o montante emprestado, calculada ao longo do prazo do empréstimo.

Tipo de Conta: Classificação da conta, que pode indicar, por exemplo, se a conta é corrente, poupança, empresarial ou outro tipo de conta financeira, com base nos serviços oferecidos.

Tipo de Transação: A classificação da transação, como por exemplo, pagamento, transferência, depósito, saque, etc., que indica o propósito e o tipo de movimento financeiro realizado.

Tipo de Acesso: A classificação do tipo de ação realizada durante o acesso, como login, logout, visualização de informações, modificação de dados, etc., indicando o propósito do acesso.

Tipo de Interação: A classificação da interação, que pode ser, por exemplo, atendimento ao cliente, reclamação, chamada, solicitação de informações, feedback, entre outros, indicando o tipo de comunicação ou ação realizada.

Tipo de Cartão: A categoria ou classe do cartão, como "Crédito", "Débito", "Pré-pago", entre outros, que define a natureza e as funcionalidades do cartão.

Telefone: Número de telefone utilizado para contato, podendo ser fixo ou móvel. Este dado é utilizado para estabelecer comunicação direta com o indivíduo ou empresa.

U

V

Valor da Transação: O montante de dinheiro que é transferido de uma conta para outra durante uma transação, que pode ser positivo ou negativo dependendo do tipo de transação.

Valor do Empréstimo: O montante de dinheiro que foi emprestado ao cliente, representando a quantia que ele se compromete a pagar de volta, com juros, conforme os termos do contrato de empréstimo.

Anexo VI - *framework* HESA

People and cultura (Pessoas e cultura)

1. Como é que a responsabilidade e a propriedade dos dados são geridas em toda a organização?

Não foram encontradas informações de como o banco gere a responsabilidade e propriedade dos dados da organização, no entanto, foi possível apurar que o banco reconhece a necessidade de uma abordagem estruturada para os dados, ainda que não tenha uma estrutura formal para esse efeito.

2. Qual é o custo e o valor dos dados e dos resultados obtidos a partir desses dados pela organização no seu conjunto?

Relativamente a este ponto, foi possível verificar que a organização reconhece que os dados são um ativo crítico para as suas operações e tomada de decisões, no entanto há lacunas na qualidade e consistência dos dados. O banco investiu em sistemas de análise e relatórios, no entanto a falta de qualidade e consistência tornam difícil a sua análise e não há uma compreensão clara dos custos de produção e valor dos dados para a organização. Isto sugere uma falta de visibilidade, tanto nos custos como na maximização do valor.

3. Como é que os dados são apresentados na organização?

A caracterização do ambiente empresarial refere claramente a inexistência de um dicionário de dados ou glossário, levando a inconsistências na sua interpretação e apresentação.

4. Existem funções específicas para as atividades de gestão de dados, por exemplo, administrador de dados, arquiteto de dados, analista de dados, criador de relatórios?

O banco já tem alguns recursos humanos alocados às atividades de gestão de dados, tais como a equipa de análise de dados, a gestão de base de dados e o Chief Information Security Officer, no entanto, não existe uma área formal de governança de dados ou papéis específicos dedicados a funções como Data Steward ou Data Architect.

5. As propostas de melhoria dos dados são patrocinadas a nível da gestão de topo?

Há alguma evidência de que a gestão de topo está consciente da importância da melhoria dos dados e apoia iniciativas específicas, como as indicadas pela consultora. Contudo, o suporte parece ser reativo e direcionado a problemas críticos, em vez de refletir um compromisso consistente e de longo prazo.

6. Os problemas e/ou riscos da gestão de dados são registados em registos auditáveis e/ou registos de riscos?

O Banco InovaData não possui uma área formal de Governança de Dados e a gestão de dados é feita de maneira reativa, com problemas sendo resolvidos à medida que surgem

7. Como é que os princípios e objetivos da gestão de dados são integrados em documentos políticos mais vastos?

O Banco InovaData não possui políticas formais de dados e que as práticas de gestão de dados variam entre departamentos, sem uma abordagem consistente ou integrada. Houve tentativas anteriores de implementar governança de dados utilizando *frameworks* como o DAMA-DMBOK, mas

essas iniciativas falharam devido à falta de adesão organizacional e à ausência de uma estratégia clara

8. Qual é a abordagem/capacidade da organização relativamente à análise de dados?

A capacidade analítica parece estar concentrada em poucas áreas e enfrenta desafios significativos para atender às necessidades operacionais e estratégicas de toda a organização.

Data activities (Atividades de dados)

9. São recolhidos dados para os quais não existe um objetivo ou valor óbvio?

Há uma clara confusão sobre o propósito e o valor de alguns dos dados coletados, com problemas de integração e má gestão resultando em recolhas duplicadas ou questionáveis em certos casos. Contudo, o banco parece ter alguma compreensão das principais fontes de dados e os seus usos mais críticos.

10. A qualidade dos dados é regularmente problemática em termos de operações frequentes e/ou repetíveis?

Os dados parecem ser corrigidos tardiamente e manualmente, com grande esforço envolvido para atingir um estado mínimo de qualidade, o que é indicativo de processos pouco maduros.

11. Existem várias cópias dos conjuntos de dados com pouca ou nenhuma reconciliação?

Embora o banco tenha alguma noção de onde os dados principais estão armazenados, não há evidências claras de um processo estruturado de reconciliação de dados ou de um modelo único para garantir a precisão e consistência dos dados em toda a organização.

12. Como é que a gestão dos metadados e dos dados de referência é utilizada na organização (se é que é utilizada)?

Não há evidência de que o banco tenha uma abordagem sistemática ou formal para gerir dados de meta e referência. O uso desses dados parece ser limitado, caso exista, e não parece haver um processo contínuo de desenvolvimento ou manutenção dentro de uma equipe dedicada ou de maneira integrada.

13. As pessoas que trabalham com os dados estão constantemente a “correr para ficarem paradas” para produzirem os resultados pretendidos?

Não há menção de automação significativa ou de processos simples que permitam ao banco lidar com eventos inesperados de forma eficiente. Pelo contrário, os problemas de governança de dados e a falta de integração entre sistemas resultam em uma constante necessidade de intervenção manual e correção de dados.

14. É dada prioridade às atividades de dados em detrimento de outras coisas que precisam de ser feitas?

Não há evidências claras de um plano de melhoria de dados formal, com um responsável claro e patrocinado por um indivíduo com autoridade. Em vez disso, as atividades de dados parecem ser tratadas de maneira reativa, lidando com os problemas à medida que surgem, como exemplificado pelos atrasos nos relatórios e a falta de um processo de governança sólido.

15. Existe um conhecimento das melhores práticas de gestão de dados e/ou de governação formal de dados?

Não há uma evidência clara de que as melhores práticas de gestão de dados sejam aplicadas de forma abrangente em toda a organização, com uma gestão sistemática e bem definida dos dados. A governança de dados parece estar limitada a tentativas iniciais sem uma implementação efetiva.

16. A organização tem um plano para melhorar a qualidade dos dados e, em caso afirmativo, como é que isso se manifesta?

O banco reconhece que a qualidade dos dados é um desafio e que a falta de padrões e governança de dados resulta em um processo manual de limpeza de dados, mas não há indicação de metas específicas ou de KPIs formais para monitorar a qualidade dos dados de maneira regular ou estruturada. Embora existam esforços para lidar com questões pontuais relacionadas à qualidade dos dados, como problemas de consistência e integração entre sistemas, esses esforços são descritos de maneira reativa.

17. Qual é o grau de segurança dos dados da organização e como é que essa segurança é mantida e auditada?

Embora haja alguma segurança no nível da infraestrutura e algumas auditorias internas, não há uma evidência clara de que o banco esteja auditado externamente ou tenha implementado um framework de segurança formalizado em todos os seus dados ou que os dados sejam marcados de acordo com um framework.

Business process (Processo empresarial)

18. A sua organização tem processos repetíveis/documentados para efetuar as operações de dados mais frequentes?

A falta de uma abordagem estruturada para governança de dados e qualidade sugere que os processos de dados, embora realizados frequentemente, não são totalmente documentados ou uniformizados de forma que possam ser repetidos de maneira eficiente e sem intervenção manual constante.

19. Como é que os processos empresariais estão alinhados com os resultados externos e as obrigações de informação?

O Banco InovaData enfrenta dificuldades significativas com a qualidade e consistência dos dados, o que tem afetado a capacidade de entregar relatórios regulatórios e conformidade de maneira eficiente. Há atrasos nos relatórios de conformidade ao Banco de Portugal, como resultado de problemas com a integração e limpeza de dados, indicando que os processos não são totalmente uniformizados ou automáticos.

20. Como é que os problemas são controlados, resolvidos e auditados?

Pelas informações presentes no caso de estudo do banco, os problemas são encontrados e corrigidos à medida que surgem, mas sem um processo formal ou framework de gestão de problemas, como evidenciado pela ausência de métricas claras de qualidade de dados e de governança estruturada.

21. Até que ponto a colaboração é transversal para reduzir os riscos/corrigir problemas com os dados?

Não há um fórum regular ou uma abordagem formalizada de colaboração entre diferentes departamentos ou funções para partilhar problemas de dados ou para trabalhar em soluções de melhoria, conforme indicado pela falta de uma governança de dados estruturada e integrada.

22. Como é que os processos de gestão de dados são integrados nos processos empresariais mais alargados?

Embora o banco tenha processos para dados em algumas áreas, esses processos não são bem integrados com os processos de negócios mais amplos. A falta de um Dicionário de Dados ou Glossário e de uma abordagem estruturada para a gestão de dados sugere que os processos de dados não estão claramente alinhados ou documentados para serem integrados de maneira eficiente com outras funções ou processos organizacionais

23. Como é avaliado o impacto da mudança organizacional em relação às capacidades atuais ou futuras de gestão de dados?

A informação disponível no documento sugere que o banco se encontra frequentemente atrasado na identificação de problemas de dados e não parece integrar a gestão de dados de maneira antecipada em projetos de mudanças, o que indica que o impacto das mudanças em dados não é sempre adequadamente avaliado de forma proativa.

O documento sugere também que, em muitos casos, as mudanças são tratadas de forma reativa, sem uma análise antecipada de como elas afetarão os dados ou a gestão desses dados.

24. Mede a qualidade dos dados? Em caso afirmativo, como define as suas métricas e quem as monitoriza?

Não há menção de métricas amplamente aplicadas a todos os conjuntos de dados ou de um processo estruturado para monitorar a qualidade dos dados de forma regular e constante, como parte de uma rotina operacional.

25. Como é que os dados apoiam a tomada de decisões baseadas em factos?

Apesar de o banco confiar em seus dados para decisões operacionais diárias, a qualidade dos dados não é garantida de forma consistente, o que significa que nem todas as decisões podem ser totalmente baseadas em dados confiáveis ou precisos.

26. Existe um processo/estratégia de continuidade da atividade para os ativos de dados?

Embora o banco tenha medidas de segurança para proteger dados, como replicação entre data centers e planos de recuperação de desastres, não há uma evidência clara de que a disponibilidade dos dados seja tratada como uma prioridade crítica dentro de um plano formal de continuidade de negócios ou que seja regularmente testada.

Technology (Tecnologia)

27. Em que medida é que a empresa em geral compreende o papel das TI na gestão e utilização dos dados?

A área de TI parece estar envolvida com a gestão dos dados, mas a relação com outras áreas de negócios parece ser mais técnica e operacional, sem uma colaboração mais profunda ou estratégica no uso dos dados para fins de transformação ou inovação.

28. Qual é a função da arquitetura de dados na sua organização (se existir)?

A função de arquitetura de dados parece não existir de forma formalizada ou estruturada no Banco InovaData, e não há uma abordagem unificada para implementar uma arquitetura de dados que suporte a transformação organizacional.

29. Como é que as soluções tecnológicas apoiam o ciclo de vida dos dados da organização (por exemplo, aquisição, limpeza, utilização, arquivo, eliminação)?

Embora haja algumas ferramentas tecnológicas em uso, como o VMware ESXi e sistemas de CRM, essas ferramentas não estão completamente integradas em uma abordagem estruturada para gerir o ciclo de vida dos dados de forma eficiente, desde a aquisição até a eliminação de dados.

30. Como é que os dados são controlados e modelados?

O banco entende a importância de modelar e dominar dados, mas a falta de uma abordagem integrada e formal de gestão de dados mestre e a fragmentação dos dados dificultam a criação de uma estrutura unificada e bem modelada para todos os dados.

Anexo VII - Política de qualidade dos dados

Objetivo

O objetivo da presente política de qualidade dos dados é estabelecer normas e práticas para garantir que os dados recolhidos, armazenados, processados e divulgados pelo Banco InovaData são exatos, fiáveis, coerentes e oportunos. Esta política apoia a tomada de decisões, a responsabilização e a prestação de serviços.

Âmbito

Esta política aplica-se a todos os ativos de dados, incluindo, mas não se limitando a, dados pessoais, dados operacionais, dados financeiros e dados estatísticos, geridos pelo Banco InovaData.

Definições

Termo	Definição
Qualidade dos dados	O grau em que os dados são exatos, completos, oportunos, coerentes e relevantes para o fim a que se destinam.
Data Steward	Um indivíduo responsável pela gestão da qualidade dos dados num domínio específico.
Data Custodian	Um guardião de dados é um indivíduo ou uma equipa dentro de uma organização responsável pela gestão técnica e proteção dos dados. Esta função engloba a implementação e manutenção de medidas de segurança de dados, garantindo a integridade, disponibilidade e privacidade dos dados. Os guardiões de dados são normalmente profissionais de TI que tratam das operações diárias relacionadas com o armazenamento de dados, controlo de acesso, cópia de segurança e recuperação
Metadados	Informação estruturada que descreve, explica, localiza ou facilita a recuperação, utilização ou gestão de um recurso de informação.

Princípios da qualidade dos dados

Os esforços de qualidade dos dados devem garantir a adesão às Seis Dimensões da Qualidade dos Dados:

- **Integralidade:** Os dados devem ser completos, contendo toda a informação necessária para a sua utilização prevista. Não devem faltar campos ou valores, exceto se estes não estiverem legitimamente disponíveis.
- **Singularidade:** Os registos ou entidades de dados devem ser distintos e não conter entradas duplicadas. A unicidade mede se cada item de dados, como um registo de cliente, ID de produto ou transação, aparece apenas uma vez no conjunto de dados ou na base de dados.
- **Atualidade:** Os dados devem estar atualizados e relevantes para a utilização a que se destinam. Devem ser recolhidos, processados e disponibilizados dentro de um prazo razoável para apoiar a tomada de decisões e a análise.
- **Validade:** Os dados devem aderir a regras, normas e restrições predefinidas. Devem ser válidos em termos do seu formato, estrutura e conteúdo, assegurando a sua conformidade com os critérios esperados.
- **Exatidão:** Os dados devem ser exatos e precisos, refletindo o verdadeiro valor ou condição que representam. Isto significa minimizar os erros, as discrepâncias e as incoerências.

- **Consistência:** Os dados devem ser consistentes em diferentes conjuntos de dados, sistemas e períodos de tempo. A consistência garante que os dados podem ser utilizados e comparados de forma fiável sem variações ou discrepâncias inesperadas.

Funções e responsabilidades

Função	Responsabilidade
Conselho de Governação de Dados	Supervisiona a gestão da qualidade dos dados em toda a organização e assegura a conformidade com esta política.
Data Stewards	Garantir a qualidade dos dados nos seus domínios, implementando normas e procedimentos de qualidade dos dados.
Departamento de TI	Apoia iniciativas de qualidade de dados através de tecnologia, ferramentas e infra-estruturas.
Todos os funcionários	Responsável pelo cumprimento das práticas de qualidade dos dados e pela comunicação de quaisquer problemas de qualidade dos dados.

Política

- Os processos de gestão da qualidade dos dados devem ser incorporados para monitorizar, medir e melhorar a qualidade dos dados trocados entre sistemas, garantindo que os dados são exatos, completos e coerentes em todos os sistemas integrados.
- Todos os sistemas devem ter normas documentadas de introdução de dados e os utilizadores devem receber formação sobre essas normas para minimizar os erros.
- As regras de validação para a introdução de dados devem ser aplicadas em todos os sistemas para garantir a exatidão e a exaustividade dos dados no ponto de entrada.
- Todos os funcionários devem ter o devido cuidado ao introduzir informações em sistemas ou formulários para garantir a sua exatidão e integridade.
- Os responsáveis pelos dados devem definir métricas e objetivos específicos de qualidade dos dados para os ativos de dados críticos do COV (por exemplo, 95%, precisão de nível 1 ou nível 2 para as informações de contacto dos clientes).
- Os Data Stewards devem definir um processo para monitorizar e comunicar os parâmetros de qualidade dos dados, com reuniões de revisão regulares (por exemplo, trimestrais).
- Os Data Stewards e os Data Custodians devem garantir a coerência ao integrar dados de várias fontes.
- Os Data Stewards devem manter metadados completos para fornecer contexto e melhorar a usabilidade dos dados.

Conformidade e auditoria

- O cumprimento desta política é obrigatório para todos os departamentos e indivíduos envolvidos na introdução e gestão de dados.
- O cumprimento desta política é obrigatório para todos os departamentos e indivíduos envolvidos na introdução e gestão de dados.
- O incumprimento pode dar origem a medidas corretivas determinadas pela direção do Banco InovaData.

- Os Data Stewards ou outros membros da equipa de auditoria devem realizar auditorias regulares para avaliar a adesão a esta política e identificar áreas a melhorar.

Formação e apoio

Os responsáveis pelos dados devem fornecer formação contínua e recursos a todos os funcionários sobre as melhores práticas e normas de qualidade dos dados e a importância de manter uma elevada qualidade dos dados.

Revisão da política

Esta política será revista e atualizada anualmente a partir da data de aprovação, ou mais frequentemente, se necessário. Os membros do pessoal que desejem fazer comentários sobre a política podem enviar as suas sugestões.

Anexo VIII - Política de integração de dados

Objetivo

A presente política tem como objetivo definir diretrizes para a integração de dados entre sistemas e serviços do Banco InovaData, promovendo a interoperabilidade, a consistência e a qualidade dos dados, enquanto garante a segurança e a conformidade com as normas aplicáveis.

Âmbito

Esta política aplica-se a todos os processos e tecnologias utilizados para a integração de dados entre sistemas internos e externos ao Banco InovaData.

Definições

Termo	Definição
Integração de Dados	Processo de combinação de dados de diferentes fontes, proporcionando uma visão unificada e consistente.
Sistema Fonte	Sistema que fornece os dados a serem integrados.
Sistema Alvo	Sistema que consome os dados integrados.
Interface de Programação de Aplicações (API)	Mecanismo utilizado para permitir a comunicação entre sistemas.
ETL (Extração, Transformação e Carregamento)	Processo de extração de dados de uma fonte, transformação para um formato adequado e carregamento no sistema alvo.

Princípios da qualidade dos dados

- **Qualidade e Consistência dos Dados:** Todos os dados integrados devem ser validados para garantir a sua integridade e precisão.
- **Interoperabilidade:** Os sistemas devem aderir a padrões reconhecidos para assegurar a compatibilidade entre diferentes plataformas.
- **Segurança:** A integração de dados deve garantir a proteção contra acessos não autorizados, utilizando medidas como encriptação e autenticação robusta.
- **Escalabilidade:** Os processos de integração devem ser capazes de suportar o aumento do volume de dados sem comprometer o desempenho.

Normas de Integração de Dados

- **APIs:** Sempre que possível, utilizar APIs baseadas em REST ou GraphQL para integração.
- **ETL:** Para grandes volumes de dados ou sistemas legados, o processo ETL deve ser documentado e seguir as diretrizes de qualidade de dados.
- **Formato dos Dados:** O formato preferencial para troca de dados é JSON ou XML. Outros formatos podem ser utilizados mediante justificativa.

Funções e responsabilidades

Função	Responsabilidade
Data Stewards	por supervisionar a qualidade e a consistência dos dados nas integrações.

Equipa Técnica	Responsável pela implementação e manutenção dos processos de integração.
Proprietário do Sistema	Deve assegurar que os requisitos de integração estão alinhados com as necessidades do negócio.

Processo de Integração

- **Planeamento:** Definir os requisitos de negócio e os sistemas envolvidos.
- **Desenvolvimento:** Configurar os processos e testar as integrações em ambiente controlado.
- **Validação:** Realizar testes para assegurar a qualidade e a segurança dos dados integrados.
- **Implementação:** Migrar os processos de integração para o ambiente de produção.
- **Monitorização:** Utilizar ferramentas para monitorizar e corrigir eventuais falhas nas integrações.

Conformidade e Revisão

O cumprimento desta política é obrigatório. A política será revista anualmente para garantir que se mantém atualizada e relevante.

Formação e apoio

Sessões de formação sobre as melhores práticas de integração de dados serão disponibilizadas pela equipa de governação de dados.

Revisão da política

Esta política será revista e atualizada anualmente a partir da data de aprovação, ou mais frequentemente, se necessário. Os membros do pessoal que desejem fazer comentários sobre a política podem enviar as suas sugestões.

Anexo IX - Políticas de Segurança dos dados

1. Objetivo

A Segurança de Dados é fundamental para assegurar a privacidade e a confidencialidade dos dados, garantindo que não sejam violados e que o acesso ocorra de forma apropriada. Os objetivos principais dessa política incluem possibilitar a propriedade dos ativos de dados da empresa, prevenir acessos inadequados a esses ativos, compreender e cumprir os regulamentos e políticas relevantes para privacidade, proteção e confidencialidade, além de assegurar que as necessidades de privacidade e confidencialidade de todas as partes interessadas sejam devidamente aplicadas e auditadas.

2. Âmbito

Esta política de segurança de dados aplica-se a todos os dados de clientes, dados pessoais e outros dados considerados sensíveis de acordo com a política de classificação de dados da empresa. Inclui servidores, bases de dados, sistemas de TI e dispositivos usados para aceder, processar ou armazenar tais dados. Todos os utilizadores que interagem com os serviços de TI da empresa estão sujeitos a esta política.

3. Políticas de Segurança dos Dados

3.1 Criptografia

Os dados devem ser encriptados para garantir que apenas utilizadores autorizados possam aceder-lhes.

3.2 Antivírus e Anti-Malware

Devem ser instalados e atualizados antivírus e anti-malware para proteger os sistemas contra software malicioso.

3.3 Atualizações Regulares

Os sistemas operativos, aplicações e dispositivos devem ser mantidos atualizados regularmente para prevenir a exploração de vulnerabilidades conhecidas.

3.4 Palavras-Passes

Devem ser usadas palavras-passe complexas para dificultar ataques baseados em credenciais, como ataques de força bruta ou ataques por dicionário. A alteração das palavras-passe é obrigatória a cada 3 meses.

3.5 Gestão de Dispositivos Móveis

Os dispositivos móveis usados para aceder a dados corporativos devem ser configurados com medidas de segurança adequadas, como encriptação e controlo de acesso.

1.1 VPNs (Redes Privadas Virtuais)

As VPNs devem ser usadas para estabelecer conexões seguras ao aceder aos sistemas corporativos a partir de redes públicas ou inseguras, garantindo a confidencialidade e integridade dos dados transmitidos

1.2 Autenticação de Dois Fatores (2FA)

A autenticação de dois fatores deve ser implementada, exigindo dois métodos independentes de verificação para o acesso aos sistemas.

1.3 Restrições ao Uso de RDP (Remote Desktop Protocol)

O uso do RDP deve ser limitado e rigorosamente gerido devido ao seu histórico de vulnerabilidades e ataques cibernéticos.

1.4 Gestão de Identidade e Acesso (IAM)

Devem ser implementados controlos rigorosos para definir quem pode aceder a quais recursos, com base em perfis de risco, funções e permissões, minimizando o risco de acesso não autorizado.

3.10 Auditorias de Segurança

Auditorias regulares devem ser realizadas para identificar vulnerabilidades e falhas de segurança. Estas auditorias devem resultar em ações corretivas ou ajustes nos controlos de segurança.

1.5 Equipamentos Fornecidos pela Empresa

Devem ser utilizados dispositivos fornecidos pela organização, configurados e controlados de acordo com as políticas de segurança da empresa.

1.6 Educação e Sensibilização dos Colaboradores

Treinamentos contínuos devem ser realizados para garantir que todos os colaboradores compreendam as melhores práticas de segurança, incluindo o reconhecimento de *phishing*, gestão de palavras-passe e proteção de dados.

4. Responsabilidades

- **Data Owners:** Responsáveis por garantir que os dados sob a sua gestão são bem cuidados. Decidem como os dados devem ser usados, quem os pode aceder, e como devem ser protegidos.

- **Administradores de Segurança da Informação**: Fornecem suporte administrativo para a implementação e coordenação de procedimentos e sistemas de segurança.

- **Utilizadores**: Incluem todas as pessoas que têm acesso aos recursos de informação, como funcionários, contratados, consultores, trabalhadores temporários e voluntários.

- **Equipa de Resposta a Incidentes**: Responsável pela identificação e tratamento de incidentes de segurança. Gere também problemas de segurança como violações de dados ou ciberataques.

5. Penalizações

Qualquer utilizador que viole qualquer uma das políticas mencionadas está sujeito a medidas disciplinares, incluindo possível rescisão do contrato de trabalho. Terceiros e contratados que não cumprirem a política podem ter as suas conexões de rede terminadas.

6. Auditoria e Revisão

A política deve ser revista regularmente para incluir novos ativos e operações. Todas as alterações devem ser documentadas no histórico de revisões.

7. Definições

- **Encriptação:** Processo de transformar dados em um formato ilegível, acessível apenas por utilizadores autorizados.
- **Autenticação de Dois Fatores (2FA):** Método de segurança que exige dois meios independentes de verificação para acesso.
- **VPN (Rede Privada Virtual):** Conexão segura que permite acesso remoto protegido a redes corporativas.
- **IAM (Gestão de Identidade e Acesso):** Sistema que controla e define permissões para acesso a recursos de informação.
- **Antivírus e Anti-Malware:** Software projetado para detetar, prevenir e remover software malicioso.

8. Histórico de Revisões

Versão	Data	Autor	Descrição das Alterações
1.0	22/01/2025	Equipa de TI	Versão inicial com políticas atualizadas