Banco do Brasil

PDTI
Plano Diretor de Tecnologia da Informação
Período 2025/2026

Julho / 2024

Sumário

1. Introdução

Este documento tem como objetivo apresentar um Plano Diretor de Tecnologia da Informação para o Banco do Brasil S. A. para o próximo biênio de 2025 a 2026.

O Plano Diretor de Tecnologia da Informação (PDTI) consiste em um documento com o objetivo de realizar o planejamento e elaborar estratégias para a área de TI. Ele especifica os processos de TI que a organização adota para administrar suas atividades e atua como um roteiro para decisões relacionadas à TI. O PDTI é essencial para orientar decisões, gerenciar recursos de TI e garantir que a estratégia de TI esteja alinhada com os objetivos da instituição.

Portanto, este documento contém o diagnóstico da área de TI, macroprocessos a serem trabalhados no período especificado neste documento, as demandas de aquisições necessárias, além de incluir um cronograma e os custos associados a todas as implementações necessárias.

2. Referencial Estratégico

2.1 Instituição

Banco do Brasil S.A.

2.2 Ramo de atividade

Instituição financeira.

2.3 Missão

“Ser próximo e relevante na vida das pessoas em todos os momentos.”.

2.4 Visão

“Ser o Banco mais relevante e confiável para a vida dos clientes, funcionários, acionistas e para o desenvolvimento do Brasil.”.

2.5 Valores

- Inovação - inovamos para simplificar as soluções e facilitar a vida das pessoas;
- Proximidade - somos presentes, proativos e empáticos para encantar as pessoas;
- Compromisso com a sociedade – consideramos o interesse coletivo na tomada de nossas decisões;
- Integridade – atuamos pautados no respeito, confiança, ética e transparência;
- Eficiência - otimizamos os recursos disponíveis para criar valor aos nossos públicos de relacionamento;
- Diversidade – promovemos a diversidade, a equidade e a inclusão para construir relações e resultados sustentáveis.

2.6 Alinhamento da TI ao Planejamento Estratégico

Com o objetivo de obter um melhor alinhamento da TI com as áreas de negócios e com o seu Planejamento Estratégico, o Banco do Brasil vai reestruturar toda a sua área de tecnologia, buscando melhorar a gestão, sua Governança de TI, valorizar o conhecimento, primar pela ética profissional e sustentabilidade, segurança, qualidade e excelência dos produtos e serviços, minimizar custos e maximizar o uso dos recursos existentes com o mínimo de investimento, inclusive auferindo lucros com a área de TI.

3. Diagnóstico

A análise SWOT é uma ferramenta de planejamento estratégico que avalia as forças, fraquezas, oportunidades e ameaças de uma empresa. Ela proporciona um diagnóstico completo da situação da empresa, considerando tanto o ambiente interno quanto o externo. Através dessa análise, é possível identificar os fatores que impactam o desempenho e a competitividade, fornecendo insights relevantes para tomada de decisões e desenvolvimento de projetos sólidos.

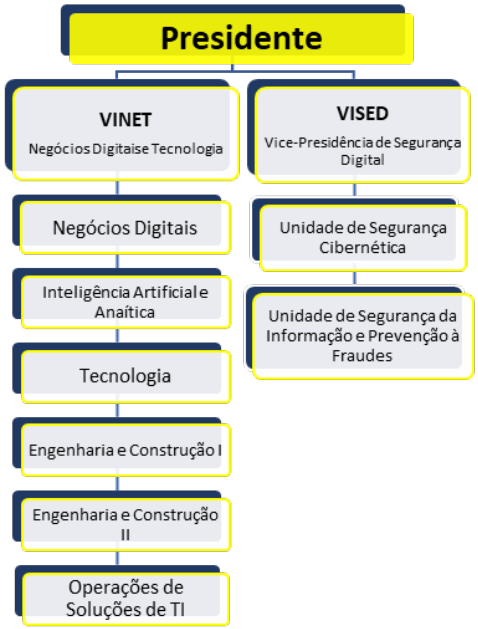
3.1 Análise SWOT da TI

Tabela 1 - Matriz Swot

Melhorar a Segurança Digital; • Possibilidade de criar parcerias; • Atrair mais clientes.	Crise econômica mundial.

3.2 Estrutura Organizacional Atual

Na situação atual, os setores de TI constantes do organograma abaixo encontram-se com uma carga de trabalho e recursos bem estruturados, mas extremamente focados no desenvolvimento e infraestrutura de TI, havendo necessidade de ajustes na estrutura organizacional para otimizar e direcionar os recursos para estratégias de segurança digital, a fim de garantir a continuidade dos negócios.



3.3 Estrutura Organizacional Proposta

No organograma abaixo foi proposta a criação de uma Vice-Presidência de Segurança Digital com respectivas unidades, gerências, atribuições. O objetivo é que a segurança da informação e cibernética tenham a mesma relevância dentro do Banco do Brasil quanto as áreas de desenvolvimento de produtos.

O Banco do Brasil deve considerar a segurança digital como uma parte fundamental de sua estratégia de tecnologia e investir recursos adequados na implementação de medidas de segurança robustas para proteger seus ativos digitais e mitigar os riscos associados à cibersegurança.

4. Planejamento do Macroprocessos Estratégicos para Área de Tecnologia

4.1 Governança de TI

A Governança de TI é um desmembramento da Governança Corporativa e abrange um conjunto de normas, práticas, ações, competências e responsabilidades necessárias para alinhar os recursos de TI à estratégia organizacional. Ou seja, a Governança de TI é um conjunto de estratégias relacionadas às políticas de governança

corporativa (baseando-se na missão, visão e valores da organização), mas com ênfase nos processos de gestão dos recursos tecnológicos, alinhada as políticas e estratégias da área de TI com as necessidades das demais áreas. Atua diretamente em Auditoria e conformidade, desempenho e indicadores, comunicação e informações, pessoas e capacitações, projetos e processos.

4.1.1 Princípios de TI

Princípios e diretrizes são considerados regras gerais que norteiam os conceitos de uma matéria, orientando a tomada de decisão. Constituem proposições estruturantes para determinado fim, ou seja, são alicerces de um assunto.

A ISO/IEC 38500 fornece seis princípios básicos de governança de TI em suas normas: responsabilidade, estratégia, aquisições, desempenho, conformidade e comportamento humano. Elas estão registradas no site da ABNT, a Associação Brasileira de Normas Técnicas:

Tabela 2 - Princípios de TI

Princípios	Detalhamento	Origem
Responsabilidade	Cada indivíduo na empresa deve entender sua responsabilidade para com a tecnologia da informação. Os responsáveis precisam ter a autoridade necessária para executarem suas ações.	ISO/IEC 38500.
Estratégia	Todas as estratégias da empresa precisam ser alinhadas com a capacidade de tecnologia que ela possui ou projeta ter.	ISO/IEC 38500.
Aquisições	As decisões por novas aquisições no setor de TI precisam ter transparência e apresentar razões válidas. Isso também leva a um melhor uso dos recursos financeiros da organização.	ISO/IEC 38500.
Desempenho	O papel da TI é dar suporte à atividade fim da empresa, oferecendo recursos e garantir qualidade para que sejam executadas as ações necessárias para atingir os objetivos da companhia.	ISO/IEC 38500.
Conformidade	É preciso haver conformidade nos processos. Eles devem seguir regras claras e bem definidas, de acordo com legislações e regulamentos estabelecidos.	ISO/IEC 38500.
Comportamento	O comportamento humano deve ser levado em	ISO/IEC 38500.

Humano	consideração no estabelecimento e aplicação de políticas, práticas e decisões de TI. Cada necessidade das pessoas no processo precisa ser respeitada.	

4.1.2 Iniciativas Estratégicas

Visando alinhar a área de TI ao planejamento estratégico da empresa, estão sendo propostas as seguintes Iniciativas Estratégicas:

Tabela 3 - Objetivos e Iniciativas Estratégicas

Objetivos Estratégicos	Iniciativas Estratégicas
OE01 – Reestruturar a área de TI	IE01- Atualizar o Parque Computacional
	IE02- Evoluir estrutura de dados e de comunicação para a área de TI
	IE03- Ampliar o desenvolvimento e manutenção de sistemas informatizados.
	IE04- Avaliar tecnologias e métodos a serem requeridos para a modernização da internet e intranet.
OE02 - Melhorar a gestão e implantar a governança de TI.	IE05- Implantar Governança de TI.
	IE06- Evoluir sistema de gestão de projetos da TI do BB.
	E07- Implantar política de gestão de RH.
OE03 - Primar pela ética profissional, sustentabilidade, qualidade e excelência dos produtos e serviços oferecidos aos clientes.	IE09- Criar Comissão de Ética
	IE10- Criar Código de Ética.
	IE11- Implantar ações de sustentabilidade.
	IE12- Implantar programa de melhoria de processos de desenvolvimento de software do Banco do Brasil.
OE04 - Aumentar e melhorar o conhecimento.	IE13- Realizar diagnóstico para melhorar o conhecimento na TI.
	IE14- Melhorar processos e implantar novas tecnologias/práticas de gestão do conhecimento.
	IE15- Implementar plano de capacitação de TI.
OE05 - Auferir lucros por intermédio da área de TI.	IE16- Criar Plano de Negócios para desenvolver novo produto ou serviço.
OE06 - Melhorar a Segurança da	IE17- Criar política de segurança da

Informação	informação para a área de TI.

4.1.3 Plano de Ação

Tabela 4 - Plano de Ação

OE	IE	Ações / Projetos	Início	Término
1	1	Levantamento do hardware e software existente	Janeiro 2025	Fevereiro2025
1	1	Decisão sobre quantidades e o que atualizar	Março 2025	Abril 2025
1	1	Contratações	Abril 2025	Abril 2025
1	2	Criar projeto para evoluir estrutura de dados e de comunicação para a área de TI	Fevereiro 2025	Abril 2025
1	3	Preparar treinamento para ampliação	Abril 2025	Abril 2025
1	3	Aplicar treinamento	Abril 2025	Novembro2026
1	4	Implantar novas tecnologias modernas	Junho 2025	Junho 2026
2	5	Preparar e aplicar treinamento sobre a Governança de TI	Junho 2025	Novembro 2026
2	6	Auditar os processos da gestão de TI	Setembro 2025	Outubro 2026
2	7	Preparar e aplicar treinamento sobre a nova política de gestão de RH	Maio 2025	Agosto 2025
3	9	Preparar e realizar reuniões com jurídico	Março 2025	Junho 2025
3	10	Disseminar na empresa código de Ética	Junho 2025	Novembro 2026
3	11	Conscientizar e promover metas	Maio 2025	Novembro 2026
3	12	Promover treinamentos e auditorias	Maio 2025	Novembro 2025
4	13	Colocar em ação melhores práticas	Maio 2025	Novembro 2026
4	14	Preparar e incentivar autoconhecimento	Fevereiro 2025	Novembro 2026
4	15	Promover treinamentos e auditorias	Fevereiro 2025	Novembro 2026
5	16	Fazer questionário com funcionários de sugestões	Fevereiro 2025	Maio 2025
6	17	Implantar política e treinamento	Janeiro 2025	Abril 2025
6	17	Disseminar informativos de alerta	Fevereiro 2025	Novembro 2026

4.2 Gestão da Segurança da Informação

4.2.1 Política de Segurança da Informação

A Política de Segurança da Informação encontra-se no Anexo II do presente documento.

4.3 Gestão do Conhecimento

4.3.1 Diagnóstico de Gestão do Conhecimento na TI

Para realização do diagnóstico sobre a Gestão do Conhecimento do Banco do Brasil foi utilizado o Método Maturidade em Gestão do Conhecimento constante de (BATISTA, 2012), onde foi verificada a pontuação constante das tabelas abaixo (itens de 1 a 42), atribuindo uma nota, conforme critérios abaixo:

Para os itens de 1 a 36 foram utilizados os valores de 1 a 5 da tabela abaixo:

Situação Atual	Escala de Pontuação
As ações descritas são muito bem realizadas	5
As ações descritas são bem realizadas	4
As ações descritas são realizadas de forma adequada	3
As ações descritas são mal realizadas	2
As ações descritas são muito mal realizadas ou ainda não são realizadas	1

Para os itens de 37 a 42 foram utilizados os valores de 1 a 5 da tabela abaixo:

Situação Atual	Escala de Pontuação
Houve melhoria em todos os indicadores utilizados	5
Houve melhoria em quase todos os indicadores utilizados	4
Houve melhoria nos resultados da maioria dos indicadores utilizados	3
Houve melhoria nos resultados de alguns indicadores utilizados	2
A organização não melhorou ou ainda não é possível comprovar melhorias por ausência de indicadores	1

CRITÉRIO 1.0: LIDERANÇA EM GESTÃO DO CONHECIMENTO		**PONTUAÇÃO**
1	A organização compartilha o Conhecimento, a Visão e a Estratégia de GC fortemente alinhados com a visão, missão e objetivos estratégicos da organização.	5
2	Arranjos organizacionais foram implantados para formalizar as iniciativas de GC (exemplos: Uma unidade central de coordenação da gestão da informação/conhecimento; Gestor Chefe de Gestão da Informação/Conhecimento; Equipes de Melhoria da Qualidade; Comunidades de Prática; e Redes de Conhecimento).	5
3	Recursos financeiros são alocados nas iniciativas de GC.	5
4	A organização tem uma política de proteção da informação e do conhecimento (exemplos: proteção da propriedade intelectual, segurança da informação e do conhecimento e política de acesso, integridade, autenticidade e sigilo das informações).	5
5	A alta administração e as chefias intermediárias servem de modelo ao colocar em prática os valores de compartilhamento do conhecimento e de trabalho colaborativo. Eles passam mais tempo disseminando informação para suas equipes e facilitando o fluxo horizontal de informação entre suas equipes e equipes de outros departamentos/divisões/unidades.	2
6	A alta administração e as chefias intermediárias promovem reconhecem e recompensam a melhoria do desempenho, o aprendizado individual e organizacional, o compartilhamento de conhecimento e a criação do conhecimento e inovação.	5
SUBTOTAL CRITÉRIO 1.0: LIDERANÇA EM GESTÃO DO CONHECIMENTO ORGANIZACIONAL - CGO		**27**

CRITÉRIO 2.0: PROCESSO		**PONTUAÇÃO**
7	A organização define suas competências essenciais (capacidades importantes do ponto de vista estratégico que concede à organização vantagem comparativa) e as alinha à sua missão e aos objetivos da organização.	5
8	A organização modela seus sistemas de trabalho e processos de apoio e finalísticos chave para agregar ("ao invés de criar") valor ao cliente e alcançar alto desempenho institucional.	5
9	Na modelagem de processos são contemplados os seguintes fatores: novas tecnologias, compartilhamento de conhecimento na organização, flexibilidade, eficiência, eficácia e efetividade para o cliente.	5
10	A organização tem um sistema organizado para gerenciar situações de crise ou eventos imprevistos que assegura a continuidade das operações, prevenção e recuperação.	5
11	A organização implementa e gerencia os processos de apoio e finalísticos chave para assegurar o atendimento dos requisitos do cliente e a manutenção dos resultados da organização.	5
12	A organização avalia e melhora continuamente seus processos de apoio e finalísticos para alcançar um melhor desempenho, reduzir a variação, melhorar produtos e serviços públicos, e para manter-se atualizada com as práticas de excelência em gestão.	5
SUBTOTAL CRITÉRIO 2.0: PROCESSO		**30**

CRITÉRIO 3.0: PESSOAS		**PONTUAÇÃO**
13	Os programas de educação e capacitação, assim como os de desenvolvimento de carreiras ampliam o conhecimento, as habilidades e as capacidades do servidor público, servem de apoio para o alcance dos objetivos da organização e contribuem para o alto desempenho institucional.	5
14	A organização dissemina de maneira sistemática informações sobre os benefícios, a política, a estratégia, o modelo, o plano e as ferramentas de GC para novos funcionários/servidores da organização.	5
15	A organização tem processos formais de "*mentoring*", "*coaching*" e tutoria.	5
16	A organização conta com banco de competências dos seus servidores públicos.	5
17	A colaboração e o compartilhamento do conhecimento são ativamente reconhecidos e recompensados/corrigidos.	4
18	A organização do trabalho contempla a formação de pequenas equipes/grupos (exemplos: grupos de trabalho, comissões, círculos de qualidade, equipes de melhoria de processos de trabalho, equipes interfuncionais, equipes interdepartamentais, comunidades de prática) e a estrutura por processos para	5

	enfrentar as preocupações e os problemas no local de trabalho.	
SUBTOTAL CRITÉRIO 3.0: PESSOAS		**29**

CRITÉRIO 4.0: TECNOLOGIA		**PONTUAÇÃO**
19	A alta administração implantou uma infraestrutura de tecnologia da informação – TI (exemplos: Internet, Intranet e site na Rede Mundial de Computadores (web) e dotou a organização com a estrutura necessária para facilitar a efetiva GC).	5
20	A infraestrutura de TI está alinhada com a estratégia de GC da organização.	5
21	Todas as pessoas da organização têm acesso a computador.	5
22	Todas as pessoas têm acesso à Internet/intranet e a um endereço de e-mail.	5
23	As informações disponíveis no site da web/intranet são atualizados regularmente.	5
24	A Intranet (ou uma rede similar) é usada como a principal fonte de comunicação em toda a organização como apoio à transferência de conhecimento e ao compartilhamento de informação.	5
SUBTOTAL CRITÉRIO 4.0: TECNOLOGIA		**30**

CRITÉRIO 5.0: PROCESSOS DE CONHECIMENTO		**PONTUAÇÃO**
25	A organização tem processos sistemáticos de identificação, criação, armazenamento, compartilhamento e utilização do conhecimento.	5
26	A organização conta com um mapa de conhecimento e distribui os ativos ou recursos de conhecimento por toda a organização.	5
27	O conhecimento adquirido após a execução de tarefas e a conclusão de projetos é registrado e compartilhado.	3
28	O conhecimento essencial de servidores públicos que estão saindo da organização é retido.	3
29	A organização compartilha as melhores práticas e lições aprendidas por toda a organização para que não haja um constante "reinventar da roda" e retrabalho.	4
30	As atividades de "*benchmarking*" são realizadas dentro e fora da organização, os resultados são usados para melhorar o desempenho organizacional e criar novo conhecimento.	5
SUBTOTAL CRITÉRIO 5.0: PROCESSOS DE CONHECIMENTO		**25**

CRITÉRIO 6.0: APRENDIZAGEM E INOVAÇÃO		**PONTUAÇÃO**
31	A organização articula e reforça continuamente como valores a aprendizagem e a inovação.	5
32	A organização considera a atitude de assumir riscos ou o fato de cometer erros como oportunidades de aprendizagem desde que isso não ocorra repetidamente.	5

33	Equipes interfuncionais são formadas para resolver problemas ou lidar com situações preocupantes que ocorrem em diferentes unidades gerenciais da organização.	5
34	As pessoas sentem que recebem autonomia dos seus superiores hierárquicos e que suas ideias e contribuições são geralmente valorizadas pela organização.	4
35	As chefias intermediárias estão dispostas a usar novas ferramentas e métodos.	5
36	As pessoas são incentivadas a trabalhar junto com outros e a compartilhar informação.	5
SUBTOTAL CRITÉRIO 6.0: APRENDIZAGEM E INOVAÇÃO		**29**

CRITÉRIO 7.0: RESULTADOS DA GESTÃO DO CONHECIMENTO		**PONTUAÇÃO**
37	A organização tem um histórico de sucesso na implementação da GC e de outras iniciativas de mudança que pode ser comprovado com resultados de indicadores de desempenho.	4
38	São utilizados indicadores para avaliar o impacto das contribuições e das iniciativas de GC nos resultados da organização.	4
39	A organização melhorou – graças às contribuições e às iniciativas da GC – os resultados relativos aos indicadores de qualidade dos produtos e serviços.	4
40	A organização melhorou – graças às contribuições e às iniciativas de GC – os resultados relativos aos indicadores de eficiência.	4
41	A organização melhorou – graças às contribuições e às iniciativas de GC – os resultados relativos aos indicadores de efetividade social.	4
42	A organização melhorou – graças às contribuições e às iniciativas de GC – a capacidade de realização dos seus objetivos estratégicos: linhas de negócio e de gestão.	4
SUBTOTAL CRITÉRIO 7.0: RESULTADOS DA GESTÃO DO CONHECIMENTO **RESULTADOS DA GESTÃO DO CONHECIMENTO**		**24**

Fonte: Adaptado da publicação da Asian Productivity Organizational (APO) – KM Facilitator's Guide.

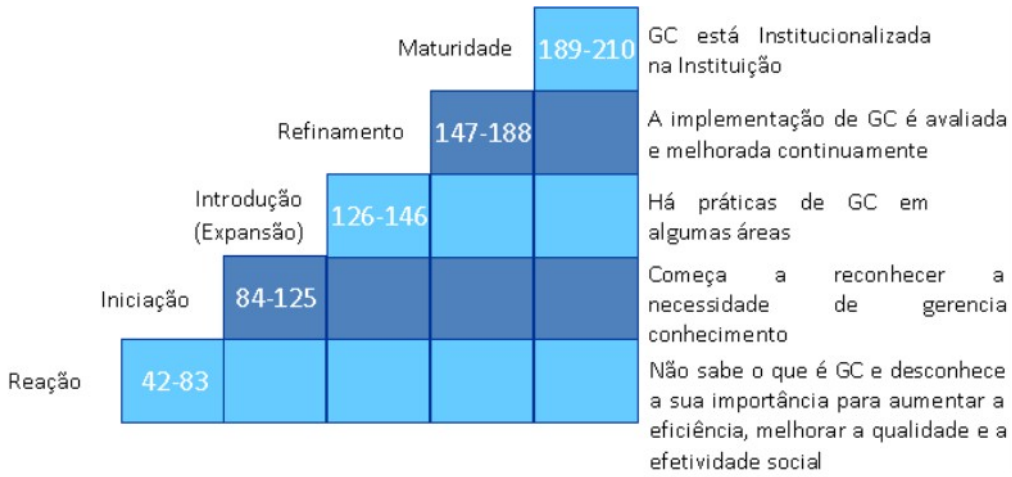
Tabela 5 - Resumo da Pontuação e Gráfico

Critério	**Pontuação por Critério Pontuação Total da avaliação (1)**		**Pontuação Máxima (2)**
1.0	Liderança em GC (Assertivas de 1 a 6)	27	30
2.0	Processo (Assertivas de 7 a 12)	30	30

3.0	Pessoas (Assertivas de 13 a 18)	29	30
4.0	Tecnologia (Assertivas de 19 a 24)	30	30
5.0	Processos de GC (Assertivas de 25 a 30)	25	30
6.0	Aprendizagem e Inovação (Assertivas de 31 a 36)	29	30
7.0	Resultados de GC (Assertivas de 37 a 42)	24	30
	TOTAL	**194**	**210**

Fonte: KM Facilitator's Guide da APO.

Figura 1 - Gráfico radar com as pontuações por critério da tabela resumo



Com base na pontuação total obtida nos critérios e conforme ilustrado na figura acima, o Método Maturidade em Gestão do Conhecimento constante de (BATISTA, 2012) ratificou a alta pontuação do Banco do Brasil, patamar – Maturidade: Gestão do Conhecimento está institucionalizada na Instituição. Desta forma, 194 pontos totais de 210 pontos representam 92% do que se poderia atingir.

4.3.2 Proposta de Processos e Tecnologias de Gestão do Conhecimento para TI

Com base no Diagnóstico constante do item 4.3.1 acima, serão implementados na área de TI os seguintes processos e práticas/tecnologias de Gestão do Conhecimento:

ORGANIZAR/ ARMAZENAR	**DISSEMINAR**
Biblioteca Virtual	Portal da Diretoria de Tecnologia - Ditec
Árvore de conhecimento	Fórum de TI

4.3.3 Mapeamento de Competências para a área de TI

Grau de Conhecimento:
N - Não necessário
B - Básico (tem noção, superficial)
D - Domina (suficiente, usa no dia-dia)
E - Especialista (larga experiência)

COMPETÊNCIAS (MÓDULOS DE FORMAÇÃO)	Vice-presidente	Gerente Geral	Gerente Executivo	Gerente de Soluções.	Gerente de Equipe	Coordenador	Especialista	Assessor TI	Assessor UE
GESTÃO									
Media Training	E	E	E	D	B	N	N	N	N
Liderança para um Mundo Exponencial	E	E	E	D	D	D	B	N	N
Líder do Futuro	E	E	E	D	D	D	D	N	N
Fundamentos de liderança de segurança para gerentes	B	B	D	D	D	D	D	N	N

Governança de TI	B	B	D	D	B	B	B	B	D
Gestão de Riscos Cibernéticos	B	B	B	B	D	D	D	B	D
ITIL v.4	B	B	B	B	B	B	B	B	N
Gestão de Projetos (PMBOK)	B	B	B	B	B	B	B	B	B
CMMI 1.3	B	B	B	B	B	B	B	B	B
SEGURANÇA DA INFORMAÇÃO									
Crise Cibernética e Continuidade de Negócios	B	B	B	D	D	D	D	B	B
Formação Executiva em Cibersegurança	B	B	D	D	D	D	D	B	B
DevSecOps	N	N	B	B	D	D	D	D	N
Segurança da Informação e Inteligência Defensiva	N	N	N	B	B	D	D	D	N
TÉCNICAS									
Ethical Hacking Python	N	N	N	B	B	D	D	D	N
Ethical Hacking Reverse Engineering Malware	N	N	N	B	B	D	D	D	N
Ethical Hacking Cloud Pentesting	N	N	N	B	B	D	D	D	N
DESENVOLVIMENTO									
Linguagens de programação	N	N	N	B	B	B	D	D	N
Java	N	N	N	B	B	B	D	D	N
Cobol	N	N	N	B	B	B	D	D	N
Python	N	N	N	B	B	B	D	D	N
Banco de Dados	N	N	N	B	B	B	D	D	N
Oracle DataBase	N	N	N	B	B	B	D	D	N
SUPORTE									
Manutenção de microcomputadores	N	N	N	N	B	B	B	D	B
Instalação e configuração de computadores	N	N	N	N	B	B	B	D	B

4.4 Ética Profissional e Desenvolvimento Sustentável

4.4.1 Ética Profissional

a) Código de Ética

O Código de Ética encontra-se no Anexo III do presente documento.

4.4.2 Desenvolvimento Sustentável

a) Educação Ambiental

Nos próximos anos deverão ser realizados os seguintes projetos:

Campanhas de Conscientização Digital: Lançar campanhas educativas em plataformas digitais que informem sobre práticas sustentáveis e o impacto das escolhas financeiras no meio ambiente. Essas campanhas podem incluir vídeos, infográficos e webinars.

Programas de Educação em Escolas: Parceria com escolas para integrar a educação financeira e ambiental nos currículos escolares, incentivando desde cedo a conscientização sobre sustentabilidade.

Workshops para Empresários e Agricultores: Organizar workshops que ensinem práticas sustentáveis específicas para diferentes setores, como agricultura, manufatura e serviços, focando em eficiência energética, gestão de resíduos e inovações verdes.

Simuladores e Ferramentas Online: Desenvolver ferramentas e aplicativos que permitam aos clientes simularem o impacto ambiental de suas escolhas de investimento, promovendo uma maior conscientização sobre as consequências de suas decisões financeiras.

b) Responsabilidade Socioambiental

Nos próximos anos devem ser realizados os seguintes projetos:

Fundo de Investimento Verde: Criar um fundo de investimento que só aplique em empresas que comprovem altos padrões ambientais e sociais, oferecendo aos investidores uma opção rentável e responsável.

Auditorias Ambientais e Sociais Regulares: Implementar um sistema de auditorias regulares para projetos financiados pelo banco, assegurando que eles continuem a cumprir os critérios ASG durante toda a sua execução.

Incentivos para Empresas com Certificações Sustentáveis: Oferecer melhores condições de crédito para empresas que possuam certificações ambientais ou de responsabilidade social, como ISO 14001 ou SA8000.

P**rogramas de Voluntariado Corporativo:** Encorajar e facilitar a participação dos funcionários em atividades de voluntariado que apoiem projetos ambientais e sociais, fortalecendo o engajamento comunitário e o compromisso dos colaboradores com a sustentabilidade.

Parcerias Estratégicas para Desenvolvimento Sustentável: Formar parcerias com ONGs, institutos de pesquisa e outras entidades para promover o desenvolvimento tecnológico e a implementação de soluções sustentáveis nas comunidades onde o banco opera.

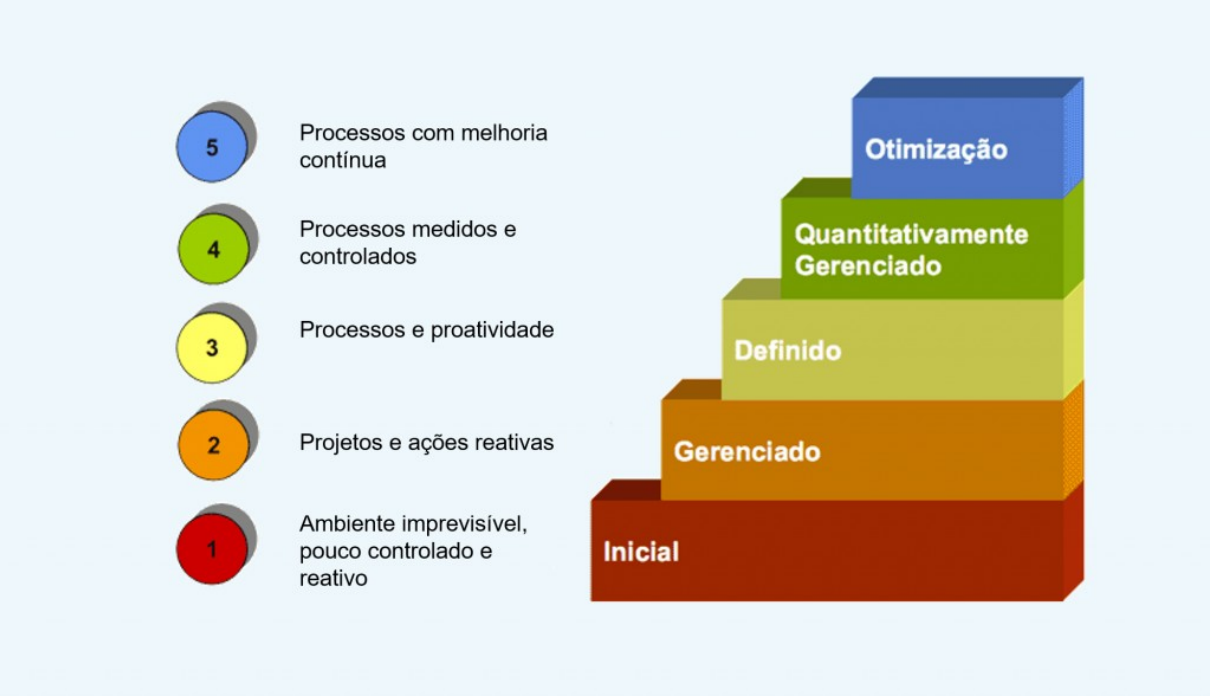
4.5 Gestão da Qualidade

4.5.1 Melhoria da Qualidade (CMMI 1.3)

O CMMI (*Capability Maturity Model Integration* ou Modelo Integrado de Maturidade em Capacitação) é um modelo de referência que contém práticas (Genéricas ou Específicas) necessárias à maturidade em disciplinas específicas SE - Engenharia de Sistemas, SW - Engenharia de Software, IPPD - Desenvolvimento Integrado de Processo e Produto, SS - Seleção de Fornecedores.

O modelo CMMI v1.3 (CMMI-DEV) contém 32 áreas de processo. Em sua representação por estágios, as áreas são divididas da seguinte forma:

O Banco do Brasil almeja alcançar o nível 3 do CMMI, mas para isso precisa implantar os seguintes processos do nível 2 do CMMI para a área de TI:



- Gerenciamento de Acordos de Fornecedores - SAM (*Supplier Agreement Management*);
- Garantia da Qualidade de Processo e Produto - PPQA (*Process and Product Quality Assurance*).

4.6 Empreendedorismo

4.6.1 Plano de Negócio para a Área de TI

O Plano de Negócio encontra-se no Anexo I do presente documento.

5. Arquitetura e Infraestrutura de TI

5.1 Atual

A infraestrutura atual depende fortemente do *backbone* central. Uma falha no *backbone* pode comprometer toda a rede. Outros problemas que podem ser observados são:

- Segurança:

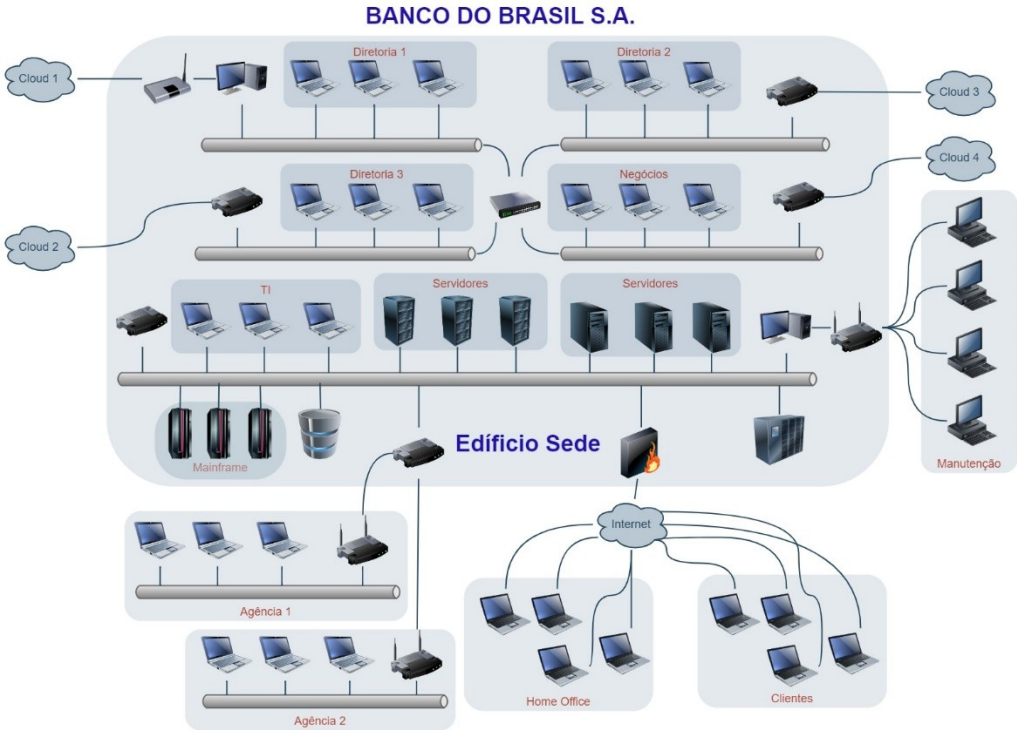
Conexões diretas com a internet para clientes e funcionários em home office podem ser pontos vulneráveis se não adequadamente protegidos.

- Desempenho:

A concentração de servidores pode criar gargalos de desempenho, especialmente se o tráfego de dados for alto.

- Escalabilidade:

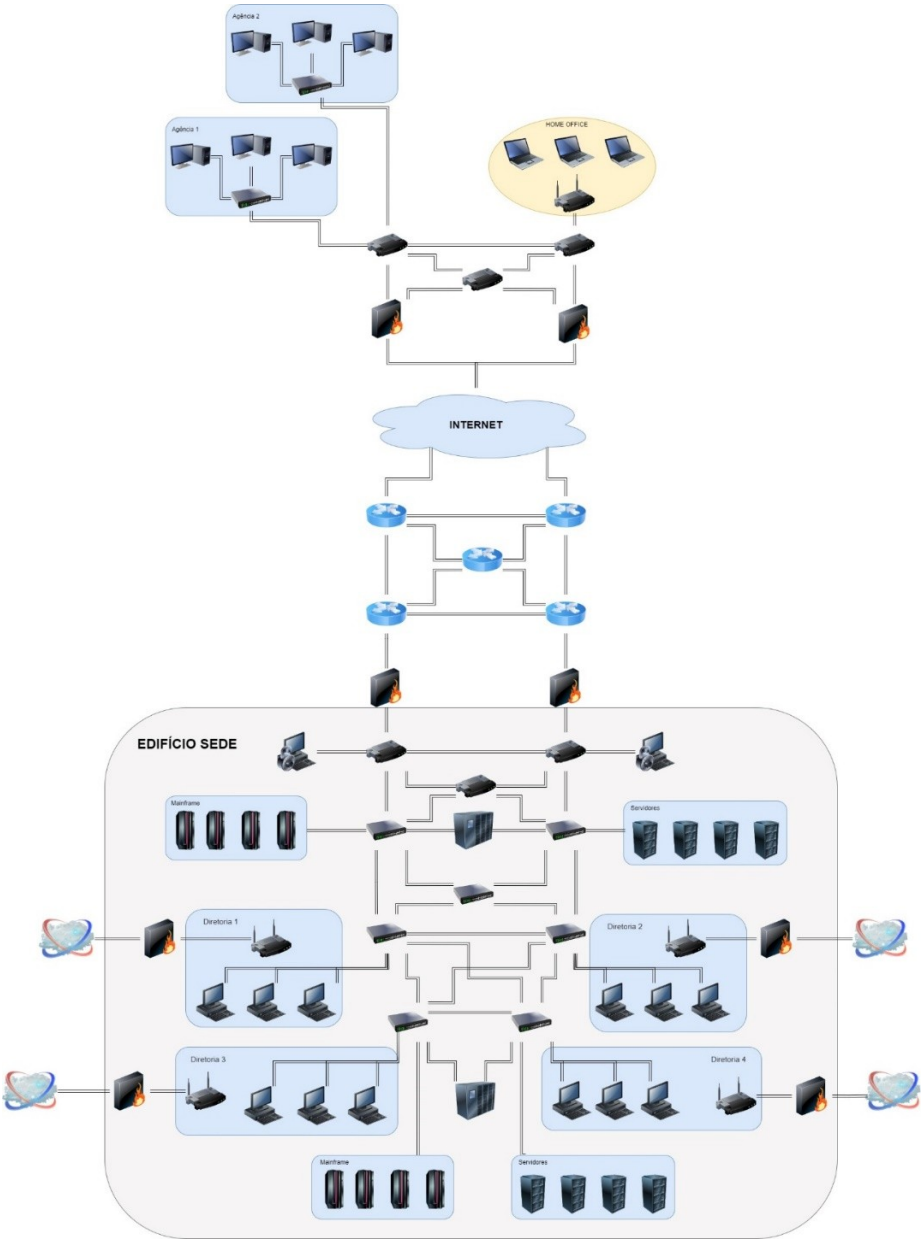
A infraestrutura atual parece ser limitada em termos de escalabilidade, especialmente com a adição de novas agências ou aumento de usuários remotos.



5.2 Proposta

A infraestrutura proposta é robusta e segura, pois garante que a empresa possa operar de maneira eficiente, segura e resiliente, minimizando riscos e otimizando o desempenho e a disponibilidade de seus serviços.

A imagem apresenta uma topologia de rede detalhada, composta por diferentes componentes e camadas que conectam uma sede principal, filiais e usuários em home office, com: estações de trabalho, roteadores, switches, firewall e racks.



6. Custos

Hardware

Item	Quantidade	Preço Unitário	Preço Total
Rack para Data Center (Dell APC Rack NetShelter SX 42U 19" 600mm x 1070mm 0)	**667**	**R$ 12k**	**R$ 8 mi**
Cabos de rede Cat 6(305m)	**1k**	**R$ 900,00**	**R$ 900k**
Subsistema de disco rígido híbrido (SSD)	**120k**	**R$ 600,00**	**R$ 72 mi**
Estação de Trabalho (Intel Core i7, 16GB DDR4, SSD de 512GB, Windows 11 Pro)	**10k**	**R$ 5k**	**R$ 50 mi**
Roteador (Cisco Catalyst 9800 Series (e.g., Cisco Catalyst 9800-40)	**20**	**R$ 40k**	**R$ 800k**
Switch (Cisco Catalyst 9300 Series)	**10**	**R$ 30k**	**R$ 300k**
Total	**131.697**	**R$88.500,00**	**R$132 mi**

Software

Item	Quantidade	Preço Unitário	Preço Total
SGBD IBM Db2	**50**	**R$ 50k**	**R$ 2,5 mi**
Firewalls para Datacenter	**12**	**R$ 2,16mi**	**R$ 26 mi**
Proteção de EndPoint Multiplataforma	**200k**	**R$ 100**	**R$ 20 mi**
Microssegmentação	**10k**	**R$ 2.500**	**R$ 25 mi**
MAST - Mobile App Security Testing	**20**	**R$100k**	**R$ 2 mi**
WAF - Web Application Firewall	**40**	**R$ 250k**	**R$ 10 mi**
Antispam	**100k**	**R$ 20,00**	**R$ 2 mi**
GRC - Governance, Risk and Compliance	**1**	**R$ 1,5mi**	**R$ 1,5 mi**
Total	**310.123**	**R$ 4.062 mi**	**R$ 89 mi**

Serviços

Item	Quantidade	Preço	Preço Total

		Unitário	
Consultoria	**1**	**R$ 750k**	**R$ 750K**
Treinamentos	**2000**	**R$ 3k**	**R$ 6 mi**
Total	**2001**	**R$753k**	**R$6.750 mi**

TOTAL GERAL.....R$ 227.750.000,00

7. Conclusão

O Plano Diretor de Tecnologia da Informação (PDTI) foi elaborado com o objetivo de realizar o planejamento e elaborar estratégias para a área de TI no Banco do Brasil, bem como prover o aumento da efetividade dos processos prestados pela área de TI. O PDTI é um importante instrumento que irá ajudar a área da TI na gestão dos recursos que estão associados as suas incumbências, como também a correta utilização dos recursos e seus descartes de forma sustentável.

Este instrumento também promove o apoio tecnológico necessário para os demais setores, visando o alcance das metas da instituição, sempre em conformidade com as leis nacionais e internacionais.

A perspectiva para as melhorias da área de TI do Banco do Brasil é para o biênio 2025/2026, sendo a partir desta data a necessária continuação das melhorias dos processos para os anos seguintes.

8. Glossário

Siglas	Descrição
BB	Banco do Brasil
PDTI	Plano Diretor de Tecnologia da Informação
TI	Tecnologia e Informação
DITEC	Diretoria de Tecnologia e Infraestrutura
SWOT	*Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças).
VINET	Negócios Digitais Tecnológicos

VISED	Vice-Presidência de Segurança Digital
ISO	*International Organization for Standardization*
IEC	*International Electrotechnical Commission*
ABNT	Agência Brasileira de Normas Técnicas
OE	Objetivos Estratégicos
IE	Iniciativas Estratégicas
RH	Recursos Humanos
GC	Gestão do Conhecimento
GCO	Gestão do Conhecimento Organizacional
UE	Unidade Estratégica
ITIL	*Information Technology Infrastructure Library*
PMBOK	*Project Management Body of Knowledge*
CMMI	*Capability Maturity Model Integration*
DevSecOps	Desenvolvimento (Dev), Segurança (Sec) e Operações (Ops
ASG	Ambiental Social e Governança
ONGs	Organização Não Governamental
SE	Engenharia de Sistemas
SW	Engenharia de Software
IPPD	Desenvolvimento Integrado de Processo e Produto
SS	Seleção de Fornecedores.
SAM	*Supplier Agreement Management*
PPQA	*Process and Product Quality Assurance*
UPS	*Uninterruptable Power Supply*
TPR	Transações com Partes Relacionadas
CGU	Controladoria Geral da União
SeCI	Sistema Eletrônico de Prevenção de Conflito de Interesses
WAF	*Web Application Firewall*
GRC	*Governance, Risk and Compliance*
MAST	*Mobile App Security Testing*

9. Referência Bibliográfica

BATISTA, Fabio Ferreira. Modelo de gestão do conhecimento para a administração pública brasileira: como implementar a gestão do conhecimento para produzir resultados em benefício do cidadão – Brasília: Ipea, 2012.

BEAL, Adriana. Gestão estratégica da informação: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2007;

CARVALHO, Marly Monteiro e RABECHINI, Roque Jr. Fundamentos em Gestão de Projetos - Construindo Competências para Gerenciar Projetos. 5ª Edição. Editora Atlas. 2018.

CRUZ, Tadeu. Sistemas, organização e métodos: estudo integrado das novas tecnologias da informação e introdução à gerência do conteúdo e do conhecimento. 3 ed.: rev. atual. ampl. São Paulo: Atlas, 2002. 276 p.: il.;

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços. 2. ed. Rio de Janeiro: Brasport, 2008. ISBN: 9788574523460. Classificação: 658:004 F363i 2. ed. Ac.3128

FONTES, Edison; Políticas e Normas para a Segurança da Informação; 1ª edição; ano: 2012; editora: BRASPORT

LAKATOS, Eva Maria e MARCONI, Marina de Andrade. Metodologia do trabalho científico. Editora Atlas. 2021.

MAGALHÃES, Ivan Luizio. Gerenciamento de Serviços de TI na Prática: Uma Abordagem com Base na ITIL. São Paulo – São Paulo: Novatec, 2007. ISBN 9788575221068. Classificação: 658:004 M188g Ac.4154.

MOLINARO, Luiz Fernando e RAMOS, Karoll Haussler Carneiro. Gestão de Tecnologia da Informação - Governança de TI: Arq. e Alinhamento entre Sistemas de Inf. e o Negócio. Editora LTC. 1ª EDIÇÃO - 2011 FERNANDES e ABREU. Implantando a Governança de TI. 4a ed. – Rio de Janeiro. Editora Brasport, 2014.

MUÑOZ-SECA, Beatriz. Transformando conhecimento em resultados: a gestão do conhecimento como diferencial na busca de mais produtividade e competitividade. São Paulo: Clio, 2004. 381 p. ISBN 8586234591.

PMBOK – 7ª Edição. 2021.

TANENBAUM, Andrew S. Redes de computadores. Rio de Janeiro: Campus, 2003. Classificação: 004.73 T164r Ac.246

Código de Ética do Banco do Brasil 2023-2024. Disponível em: https://www.bb.com.br/docs/portal/dipes/Codigo_de_Etica.pdf?pk_vid=f9c9b1f4ca08e2c11712926044dfe0ed. Acesso em: 27 abril. 2024.

ISO, Londres. Disponível em: www.iso.org/iso/home/about.htm. Acesso em: 27 abril. 2024.

CMMI, Disponível em: http://cmmiinstitute.com/#home. Acesso em: 27 abril. 2024.

Paper CI 9., Disponível em: https://abrainc.org.br. Acesso em: 19 maio. 2024.

Demonstrações Contábeis Individuais e Consolidadas – Banco do Brasil S.A., Disponível em: https://ri.bb.com.br/informacoes-financeiras/central-de-resultados/. Acesso em: 24 maio. 2024.

10. Assinaturas

10.1 Equipe Técnica Responsável

Responsáveis	Assinaturas
Fabiane Moreno	
Jéssica Simas	
Lusianna Soares	
Vinícius Simon	

10.2 Diretor de TI

Diretor de TI	Assinatura
Gerson Gimenes	

ANEXOS

Anexo I – Plano de Negócios da TI

Plano de Negócios

1. Institucional

1.1 Nome da empresa

Banco do Brasil S.A.

1.2. Caracterização da empresa

O Banco do Brasil é a maior instituição financeira do país em termos de ativos e número de clientes. Ele oferece uma ampla gama de serviços bancários, que incluem: empréstimos, investimentos, seguros e operações de câmbio. Atende diversos segmentos, desde pessoas físicas até grandes empresas e órgãos governamentais, com uma rede de agências presente em todo o território nacional.

2. Produto/Serviço

Criação de um simulador de crédito imobiliário para não correntista e correntista:

O simulador estará disponível online no site oficial do Banco e permitindo que pessoas físicas correntistas e não correntistas calculem os valores das parcelas e as condições de financiamento para a compra de imóveis.

3. Mercado e Consumidores

3.1 Consumidores Potenciais (Clientes)

Pessoa física correntista e não correntista.

Os clientes potenciais para financiamento imobiliário são diversos, abrangendo diferentes perfis e necessidades. Entre os principais grupos de clientes potenciais estão: servidores públicos, empregados do setor privado, profissionais liberais e autônomos, militares, aposentados e pensionistas, jovens e participantes de programas habitacionais.

Pessoas físicas acima de 18 anos que possuem comprovação de renda são elegíveis para o financiamento imobiliário pelo Banco do Brasil.

3.2 Tamanho do Mercado e Proposta de Valor

No Brasil, o mercado de financiamento imobiliário é significativo e tem crescido ao longo dos anos, impulsionado por diversos fatores, incluindo políticas governamentais, condições de crédito e demanda por moradia.

Segundo estimativas do estudo, a demanda habitacional no Brasil deve crescer cerca de 1,2% ao ano nos próximos 10 anos, ou mais 9 milhões de moradias. Considerando a distribuição da demanda, apenas 7% serão atendidos por subsídios e 30% por recursos com taxas regulados advindos do FGTS, mas a grande maioria, isto é, aproximadamente 63%, será financiada pelo mercado. (Paper CI 9 (abrainc.org.br)).

O simulador de financiamento imobiliário do Banco do Brasil tem como objetivo principal ajudar os clientes a entenderem melhor as condições de um possível financiamento para a compra de um imóvel. Ele proporcionará uma simulação detalhada das parcelas mensais, dos juros, do valor total financiado e outras informações relevantes, permitindo que os clientes avaliem diferentes cenários antes de tomar uma decisão de compra.

4. Concorrência

4.1 Empresas e Produtos Concorrentes

O Banco do Brasil tem cada dia mais concorrentes que investem em suas plataformas para cativar o cliente e facilitar a aquisição de um crédito imobiliário através de um bom e prático Simulador de Crédito Imobiliário. Além das taxas competitivas bancos como: a Caixa Econômica Federal, Banco BRB, Banco Inter, além dos tradicionais Bradesco e Santander, etc., todos tem bons simuladores que são fortes concorrentes ao BB.

5. Plano de Marketing e Vendas

Serão executadas ações de divulgação em todas as mídias digitais (TV canais abertos e fechados, sistema de rádio, redes sociais, Youtube e e-mails para correntista anunciando a nova plataforma para Crédito Imobiliário com mais facilidade na simulação e contato direto pelo aplicativo, WhatsApp e físico nas agências (central de atendimentos) para esclarecimento de dúvidas. A intenção será de atingir o público de todas as classes sociais.

A pesquisa de mercado será nas plataformas de simulação das instituições financeiras atuantes no mercado nacional, observando as melhores práticas que cada plataforma oferece, a fim de que no Simulador de Crédito Imobiliário do Banco do Brasil o cliente navegue com facilidade, agilidade e consiga sanar suas dúvidas e comparativos já na simulação.

6. Operações/Etapas

Etapa 1 - Pesquisa dos consumidores por serviços de simulação de crédito imobiliário disponíveis.

Etapa 2 - Formalização da intenção de desenvolvimento do simulador de crédito imobiliário.

Etapa 3 – Contato com a equipe de desenvolvimento da instituição pessoalmente ou online.

Etapa 4 - Confirmação, pela equipe de DevSecOps, da recepção do pedido e análise de requisitos.

Etapa 5 – Desenvolvimento do serviço e processamento do pedido do cliente com emissão de documentação.

Etapa 6 - Encaminhamento do pedido para entrega ao cliente.

Etapa 7 - Recebimento pelo cliente do pedido, conferência e aceitação do serviço.

Etapa 8 - Avaliação da satisfação do consumidor.

7. Planos e Projeções Financeiras

Para a implantação do Simulador de Crédito Imobiliário, serão necessários 5 (cinco) funcionários da TI internos que estarão responsáveis pelo desenvolvimento deste software. Será utilizada a infraestrutura atual para o suporte do software, com custos somente de desenvolvimento e mão de obra, tendo em vista que a utilização deste software possui chances mínimas de causar eventuais problemas de desempenho na infraestrutura já presente no Banco.

Posição	Qnt.	Salário Mensal (R$)	Salário Total (6 meses) (R$)	Custo Total (6 meses) (Proventos + Impostos) (R$)
Gerente de Soluções	1	23.000,00	138.000,00	276.000,00
Assessor I de TI (Dev. Backend)	2	15.000,00	180.000,00	360.000,00
Assessor II de TI (Dev. Frontend)	1	12.000,00	72.000,00	144.000,00
Assessor II de TI (DBA)	1	12.000,00	72.000,00	144.000,00
Total	5		462.000,00	924.000,00

Item	Valor estimado (R$)	Justificativa
Licenças de Software	3.000,00	Ferramentas de desenvolvimento (IDEs, plugins, etc.)
Infraestrutura (servidores, VMs)	2.000,00	Configuração e manutenção da infraestrutura de teste
Treinamento	1.500,00	Capacitação em tecnologias específicas (React, Java, etc.)
Testes e QA	2.000,00	Ferramentas e serviços de teste automatizado

Outros custos operacionais	1.500,00	Despesas gerais (comunicação, equipamentos, etc.)
Total Adicionais	10.000,00	

Categoria	Custo Total (R$)
Salário (6 meses)	924.000,00
Custos adicionais	10.000,00
Total Geral	934.000,00

ROI (Retorno sobre Investimento):

O Banco do Brasil, de acordo com o Balancete publicado em maio de 2024, teve valor de faturamento em financiamento imobiliário do 1º trimestre de 2024:

- Financiamentos imobiliários em milhões: R$ 55.040.491,00.

Estimativa aproximada para ano de 2024 em milhões: R$ 222.000.000,00 em financiamentos. Com o novo sistema, estimativa de aumento de 10% de lucratividade anual: R$ 22.000.000,00. Obtendo de custo para implantação do novo sistema: em torno de R$ 155.666,67 mensal, por 6 meses fica em torno de: R$ 934.000,00.

Conclusão: No primeiro mês de utilização do novo sistema o investimento já será pago, pois os 10% de aumento no faturamento mensal corresponderá a R$ 1.833.333,33 aproximadamente.

8. Análise de Riscos

RISCO	PROBABILIDADE	IMPACTO	CONTINGÊNCIA
Atraso no cronograma do projeto	2	2	Estabelecer multas e verificar periodicamente o desenvolvimento do simulador de crédito imobiliário.

Falta de recursos para o projeto	3	1	Possuir outros fornecedores para eventualidades.
Falta de orçamento	2	1	Buscar reequilíbrio nos contratos firmados.

Legenda: PROBABILIDADE (1 - Alta, 2 - Média e 3 - Baixa)
IMPACTO (1 - Alto, 2 - Médio e 3 - Baixo)

9. Tecnologias

De acordo o padrão já pré-estabelecido das tecnologias utilizadas para as aplicações web da instituição, o desenvolvimento do Simulador de Crédito Imobiliário utilizará a linguagem Java em seu *backend* para o processamento dos dados necessários e será integrada com o banco de dados Oracle. Já para o *frontend*, será feito em React.

Acessibilidade

O aplicativo será acessado pela web, portanto qualquer dispositivo que possuir um navegador com acesso à Internet poderá acessá-lo pois sua interface deve ser responsiva.

Servidor

Será utilizado os servidores já disponíveis na instituição.

Disponibilidade

O acesso estará disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

Segurança

Para controle de acessos ao servidor será utilizado o Active Directory. Os dados do usuário inseridos durante a simulação serão criptografados.

10. Assinaturas

Responsáveis	Assinaturas
Fabiane Moreno	
Jéssica Simas	
Lusianna Soares	
Vinícius Simon	
Diretor de TI	
Gerson Gimenes	

Anexo II – Política de Segurança da Informação

Política de Segurança da Informação e Cibernética do Banco do Brasil S.A.

1. Objetivo

Definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio e local em que ela esteja contida, com base na legislação vigente, órgãos reguladores, autorreguladores e nas boas práticas de segurança da informação.

2. Responsabilidade

Esta Política é de reponsabilidade do Diretoria de Riscos do Banco do Brasil. Quaisquer mudanças nesta Política devem ser aprovadas pela Diretoria de Riscos do Banco do Brasil.

A alta gestão tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

Essa política se aplica a todos os colaboradores, fornecedores e prestadores de serviços que utilizem ou forneçam serviços tecnológicos relevantes.

3. Público alvo

Esta Política se aplica a todas as instituições do Banco do Brasil.

4. Diretrizes gerais

4.1 Tratamento da Informação:

A informação sob custódia de qualquer instituição do Banco do Brasil, mesmo que pertencente a clientes, colaboradores ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

O acesso, geração, utilização, classificação, modificação, distribuição, transferência, armazenamento e eliminação da informação devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados. As instituições do BB reservam-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.

Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

A informação deve ser armazenada, pelo tempo determinado pela instituição, legislação ou regulação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

4.2 Acesso à Informação

O uso de redes externas de comunicação (Internet, redes privadas etc.) deve ser controlado através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por prestadores de serviço, deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo–se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada.

Adicionalmente, quando o acesso externo for realizado com o propósito de Home Office, deve ser observada e seguida a Política de Home Office disponível na Int ranet.

A remessa de dados da organização, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

4.3 Sistemas Aplicativos

Sistemas aplicativos desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

Sistemas aplicativos desenvolvidos fora da organização, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.

O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de atividades críticas do sistema. Onde for impraticável implantar a segregação, outros controles como monitoração das atividades, trilhas de auditoria e acompanhamento gerencial devem ser considerados.

Para minimizar o risco de falhas nos sistemas, deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos. Para novos sistemas os requisitos operacionais devem ser documentados e testados antes da sua aceitação e uso. Para sistemas já em uso devem ser feitas projeções da demanda de recursos e da carga da máquina futura a fim de reduzir o risco de indisponibilidade por sobrecarga (Capacity Planning).

5. Diretrizes específicas

5.1 Tratamento da Informação

Para o conjunto de informações utilizado por um sistema aplicativo, o Comitê Diretivo de Segurança e Contingência deve designar dois proprietários, diretores do Conglomerado, sendo um deles representante da área operacional e o outro da área de negócios.

São atribuições dos proprietários das informações:

i. Nomear o gestor das informações, a quem cabe propor as regras de acesso às referidas informações, e administrá-las operacionalmente; e
ii. Aprovar as regras de acesso às informações, conforme proposta do gestor.

Cada gestor de informações indicará um gestor substituto, a ser aprovado pelos proprietários, que deverá exercer suas funções em caso de ausência.

Cada gestor da informação e seu substituto receberão um login diferenciado para exercer esta função, ou seja, configurar os sistemas para atender às normas abaixo descritas para tratamento da informação, bem como a concessão de acessos a usuários.

i. <u>Normas para tratamento da informação</u>

Devem ser definidas regras claras para proteção da informação contra perda, alteração, acesso por pessoas não autorizadas, trilha e logs de atividade e

rastreabilidade, seja qual for o meio em que vier a ser armazenada (eletrônico, magnético, impresso etc.).

Devem ser claramente definidos os usuários (empresas, áreas, pessoas etc.) das informações, os direitos que cada um tem para acessá-las e os procedimentos para protegê-las do acesso por pessoas não-autorizadas, independentemente da forma como estiver disponível.

Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo da empresa.

Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda.

Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização.

É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade das Instituições, utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização da Diretoria responsável, e das quais os colaboradores venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

Os usuários devem adotar a prática de classificação da informação com o objetivo de fornecer o tratamento adequado à informação no aspecto de sua confidencialidade.

ii. Recomendações para o tratamento da informação

A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco.

As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da empresa.

Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área sempre que esse equipamento estiver em uso ou logado com a credencial do colaborador que necessita do suporte. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações neles contidas deverão ser destruídas antes da liberação do equipamento.

Os gestores devem determinar as regras de acesso e distribuição das informações, considerando os seguintes itens:

a. Riscos inerentes às informações:

- Acesso por pessoas não autorizadas;
- Alteração, utilização, classificação, modificação, distribuição, transferência armazenamento ou eliminação indevida; e
- Indisponibilidade.

b. Consequências:

- Fraudes: Possibilidades de lesarem as instituições do BB ou terceiros (clientes, fornecedores etc.);
- Problemas legais: Possibilidades de gerar prejuízos, multas, penalidades ou embaraços às Instituições, Diretores e Colaboradores do BB, a outras pessoas físicas ou jurídicas;

- Perda de negócio: Possibilidade de não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;

- Prejuízo de imagem do BB: Possibilidades de prejudicar a imagem do Banco do Brasil ou de seus colaboradores;

- Problemas de recuperação: Possibilidades de gerar custos de recuperação de informações perdidas ou danificadas.

5.2 Segurança quanto às Pessoas

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos do BB.

i. Identificação das pessoas:

Todas as pessoas com acesso aos sistemas e informações, pertencentes ou em posse do BB, deverão ter uma única identificação (login). As exceções deverão ser devidamente documentadas e aprovadas pelo Comitê responsável.

ii. Declaração de Responsabilidade:

É um compromisso de responsabilidade direta do colaborador para com as informações, equipamentos e outras propriedades do BB a ele confiadas, devendo ser lida e assinada quando de sua admissão.

Este conceito deve ser utilizado também para prestadores de serviço e clientes:

- Prestadores de Serviço: a declaração de responsabilidade deve ser uma das cláusulas do contrato.

- Clientes: a declaração de responsabilidade deve ser uma das cláusulas do termo de adesão ao produto - ou documento equivalente, se ao cliente for entregue alguma senha de acesso às informações.

A declaração de responsabilidade deve ser lida e assinada, dentro dos formatos aceitos e homologados em meio físico ou eletrônico, por todos os colaboradores antes de ser arquivada na respectiva pasta funcional. O Departamento de Recursos Humanos deve garantir que todos os colaboradores tenham sua declaração de responsabilidade assinada.

5.3 Segurança Lógica de Computadores, Redes e Sistemas Aplicativos

Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse do BB.

.

Todo sistema aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão etc.

Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação.

Caso as operações e suas respectivas informações envolvam quantias, poderão ser criadas alçadas, que definem a quantia máxima envolvida em operações executadas por cada classe de usuários.

As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, alçadas e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

i. Normas para segurança lógica de computadores e redes:

Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada negócio, devem estar claramente definidos e documentados e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles.

Cada gestor da informação é responsável por definir e manter atualizados os perfis de acesso aos seus aplicativos visando o acesso mínimo necessário para a execução das atividades bem como evitar conflitos de interesse.

ii. Administração do acesso aos sistemas aplicativos:

As informações devem ser analisadas pelos respectivos gestores da informação, de forma a permitir que sejam definidas as regras de acesso, através de perfis e alçadas.

Os sistemas aplicativos devem possuir recursos que possibilitem a administração dos acessos, através dos perfis e alçadas definidos pelos respectivos gestores da informação.

iii. Administração do acesso de usuários:

Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários, respeitando normas internas do BB.

iv. Controle de acesso a computadores e redes:

Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto.

O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou

rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.

Os ambientes de produção, homologação e desenvolvimento devem estar segregados entre si, de forma a impedir acessos indevidos.

v. Normas para controle de acesso a computadores, redes e sistemas aplicativos:

Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais características desse controle são:

- O acesso a computadores e redes deve ser protegido por senha;
- As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);
- Os sistemas devem ser programados para nunca exibir a senha na tela;
- As senhas devem ser individuais e intransferíveis. A senha é de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;
- As senhas não devem ser triviais e previsíveis;
- Os tipos de caracteres utilizados para a formação da senha devem ser:

1. Letras maiúsculas;
2. Letras minúsculas;
3. Números;
4. Sinais ou símbolos especiais (Ex: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ?!).

- As senhas deverão ter um tamanho mínimo de 08 (oito) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres acima definidos, sendo mandatário o uso de no mínimo um sinal ou símbolo especial;
- Os sistemas devem prever um prazo para a expiração de senhas de no máximo 30 (trinta) dias;

- Caso algum sistema defina uma senha inicial, deverá obrigar o usuário a alterá-la no primeiro acesso;

- As senhas trocadas ou expiradas devem ser cadastradas para efeito de bloqueio de reutilização (mínimo de vinte e quatro senhas);

- Os arquivos de senhas devem ser criptografados e gravados separadamente dos arquivos de dados, em ambiente de acesso restrito;

- Após um máximo de cinco tentativas consecutivas sem sucesso, os acessos devem ser bloqueados até que seja solicitado o desbloqueio do usuário; e

- Uma vez aprovada, a senha deve garantir acesso exclusivo do usuário na estação de trabalho. Portanto, um mesmo usuário não deverá utilizar simultaneamente mais de uma estação de trabalho.

vi. Monitoramento de uso e acesso aos sistemas aplicativos:

Todos os sistemas aplicativos deverão:

- Detectar tentativas de acesso não autorizado;

- Registrar eventos de entrada no sistema (login);

- Sempre que houver riscos que afetem o negócio devem ser gravadas trilhas de auditoria para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas; e

- Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

vii. Processo de desenvolvimento de sistemas:

Os sistemas desenvolvidos deverão observar e seguir as boas práticas de mercado sobre desenvolvimento seguro a fim de mitigar riscos e vulnerabilidades comumente exploradas nos sistemas. A aderência do processo deve ser realizada através de adequação de processos e/ou uso de tecnologias específicas para esse tipo de finalidade.

Adicionalmente, cabe à Segurança da Informação avaliar a necessidade de testes de segurança sobre qualquer sistema, seja interno, exposto na internet, hospedado fora da infraestrutura tecnológica do Alfa, desenvolvido internamente ou externamente.

5.4 Segurança no Acesso de Prestadores de Serviço

Este tópico visa estabelecer controles sobre recursos de processamento da informação da organização durante a execução de serviços por contratados externos.

Deve ser feita uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários. O que for acordado deve ser explicitado no contrato assinado.

É proibida a utilização de equipamentos próprios do prestador conectados à rede da organização sem a devida autorização escrita pela área de segurança da informação que deverá avaliar a necessidade através de justificativa técnica. Se for necessário deve-se segregá-los em uma rede própria e estabelecer um “firewall” para controlar os acessos.

Caso o prestador utilize softwares próprios em equipamentos da organização, deve-se apresentar documentação ou termo de responsabilidade garantindo direito de uso, que será mantido enquanto o software estiver instalado.

5.5 Segurança Física de Computadores

Este tópico destina-se aos usuários e administradores de computadores conectados ou não a uma rede.

O objetivo é garantir que as Instituições estabeleçam, administrem e utilizem computadores de maneira segura, e que sejam tomadas medidas adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos.

i. Normas para segurança física de computadores:

Os meios de armazenamento considerados como mídias removíveis devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

Os computadores não ligados a uma rede, e que contenham informações importantes para os negócios da empresa, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

Os usuários ligados a uma rede, e que tratam com informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

ii. Responsabilidade na segurança física de computadores:

A Ditec é responsável por elaborar e manter atualizado o inventário de hardware e software no Edifício Sede, Agências e Regionais.

A área de Segurança Patrimonial é responsável por garantir o controle sobre o acesso físico aos equipamentos.

5.6 Padrões para Instalação de Computadores

O padrão de instalação para os computadores deve atender a todas as normas estipuladas pelo BB.

A estrutura para manter a segurança física deve obedecer aos padrões de segurança geral do Conglomerado e adequar-se às seguintes especificações:

i. Sala:

- As dimensões do local devem ser suficientes para a instalação dos equipamentos;

- A disposição dos cabos lógicos e de energia deve ser adequada de forma que as pessoas possam transitar livremente;

- As entradas de ar (ventilação) dos equipamentos não devem estar obstruídas; e

- Os equipamentos devem estar em locais firmes que evitem trepidações.

ii. Refrigeração e qualidade do ar:

- Climatização deve ser conforme especificado pelo fabricante; e

- O ambiente deve estar livre de poluição por poeira, gases ou fumaça a fim de evitar que a poluição penetre nos equipamentos, possibilitando a quebra dos mesmos ou falhas de processamento.

iii. Rede elétrica:

- É recomendável que exista aterramento exclusivo para os equipamentos e que os pontos de energia sejam estabilizados;

- Para os equipamentos considerados críticos recomenda-se a instalação de UPS (Uninterruptable Power Supply), fonte alternativa de alimentação de energia que é ativada automaticamente quando ocorre a queda na alimentação de energia;

- Os equipamentos devem ser instalados em uma rede elétrica seguindo os padrões recomendados pelos fabricantes; e

- As instalações elétricas devem sofrer revisões periódicas.

iv. Equipamentos Contra Incêndio:

- Devem existir equipamentos de combate a incêndios adequados para materiais eletrônicos, tais como extintores de CO2, e estes devem estar em local visível sinalizado e desobstruído, e ser de conhecimento de todos os colaboradores; e

- Devem existir equipamentos de prevenção de incêndios adequados, tais como detectores de fumaça e alarme contra incêndio, devendo existir um meio eficiente de aviso a um órgão de combate a incêndio.

v. Iluminação:

- A iluminação deve ser adequada, evitando a incidência direta da luz do sol sobre os equipamentos.

vi. Precauções quanto à disponibilização das mídias de armazenamento:

- Quando as mídias removíveis de armazenamento forem vendidas, devolvidas ao fabricante ou enviadas para manutenção, as informações nelas contidas devem ser destruídas antes de deixar as dependências do BB.

Importante ressaltar que nos meios magnéticos não é suficiente apagar os dados, devendo-se executar um programa que realmente os destruam.

5.7 Segurança Física dos Servidores de Rede

Este item destina-se aos usuários de sistemas operacionais com características de servidores de rede.

O objetivo é garantir que o Conglomerado administre e utilize os diversos sistemas operacionais de maneira segura, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento.

i. Normas para segurança física dos servidores de rede:

As mídias removíveis de armazenamento devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

Os servidores de arquivos devem estar instalados em uma área que garanta a segurança física destes equipamentos incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

ii. Responsabilidades na segurança física dos servidores de rede:

A Ditec é responsável por:

- Elaborar e manter atualizado o inventário de hardware e software; e
- Garantir o controle de acesso físico aos equipamentos.

5.8 Padrões para Instalação dos Servidores de Rede

O padrão de instalação para servidores de rede deve atender a todas as normas estipuladas pelo BB.

A estrutura para manter a segurança física dos equipamentos de uma rede deverá adequar-se às mesmas especificações utilizadas para a instalação de computadores com as seguintes especificações adicionais:

i. Sala:
- Fechada, mas permitindo a visualização interna do ambiente, com divisórias até o teto.

ii. Rede elétrica:
- Nos servidores, fazer uso de equipamento UPS (homologado por técnicos autorizados) com nobreak; e
- É necessário que exista aterramento exclusivo para os equipamentos e estabilização dos pontos de energia elétrica.

iii. Equipamentos Contra Incêndio:

No caso das salas de servidores e/ou telecomunicações deve-se considerar o uso de dispositivos automatizados de combate a incêndios, agentes extintores limpos como gases e outros recursos específicos a este tipo de ambiente.

iv. Precauções quanto à disponibilização dos meios de armazenamento:

As manutenções mídias removíveis, realizadas no próprio local, devem ser acompanhadas pelo responsável da área.

5.9 Backup e Restore

Este tópico se destina aos usuários e administradores locais das empresas do BB, visando administrar e utilizar os recursos de informática de maneira segura, tomando medidas adequadas que garantam recursos alternativos de processamento na eventualidade de perda dos dados, softwares ou sistemas.

Para a elaboração de um plano de backup devem ser considerados os "backups" do tipo Operacional, Contingencial e Histórico.

Backup Operacional: é a cópia das informações estratégicas que fazem parte do quotidiano do usuário e que são importantes para garantir a continuidade de suas tarefas. Destina-se à recuperação instantânea.

Backup Contingencial: é a cópia das informações sensíveis, softwares e sistemas vitais à continuidade dos negócios do BB e deve ser guardado em local externo. Destina-se a permitir a recuperação em situações catastróficas.

Backup Histórico: é a cópia das informações determinadas por exigência legal ou normas internas e deve ser guardado em local externo.

i. Normas para Backup/Restore:

A elaboração do plano de Backup/Restore deverá levar em consideração os aspectos abaixo:

- Os períodos de atualização dos dados; e
- Particularidades de cada instituição do BB.

As informações consideradas imprescindíveis devem estar presentes nas rotinas de backups operacional e contingencial, levando-se em consideração a periodicidade de atualização dos dados.

As informações devem estar sujeitas às rotinas de backups operacional e contingencial conforme critério definido pelo usuário.

As cópias de backup devem estar guardadas em local apropriado e seguro, e protegidas contra o acesso por pessoas não autorizadas.

Deve-se manter uma cópia do plano de Backup/Restore juntamente com o backup contingencial.

Devem ser realizados testes de restore periodicamente, mantendo evidências do último teste realizado.

Devem ser mantidas, no mínimo, as duas últimas versões dos backups operacional e contingencial. Para os backups históricos, a quantidade de versões será determinada por exigência legal ou norma interna.

ii. Plano de Backup/Restore - Conteúdo:

Abrangência: Relação dos arquivos e diretórios a serem copiados no processo de backup.

Periodicidade: Intervalo de tempo após o qual o sistema é submetido à rotina de backup.

Retenção: Prazo pelo qual os backups devem ser mantidos.

Procedimentos: Descrição dos procedimentos de backup.

Quantidade de cópias: Número de cópias de backup, locais e meios de armazenamento.

Identificação dos meios de armazenamento: Os meios de armazenamento devem estar devidamente identificados.

Registro do uso das cópias de backup: A manipulação dos meios de armazenamento deve ser registrada e controlada. Estes registros devem ser guardados por 90 (noventa) dias para futuras verificações.

Manutenção das cópias Backup: Quando o prazo de retenção for superior ao especificado pelo fabricante para utilização do meio de armazenamento, deve-se adotar um procedimento para regravação dos dados em novo meio, periodicamente.

A responsabilidade do backup/restore é do administrador local ou da área técnica elaborar, manter e documentar o plano de backups e garantir a execução de seus procedimentos.

5.10 Testes regulares de armazenamento e recuperação de dados

Todo e qualquer meio de armazenamento assim como os procedimentos de recuperação devem ser regularmente testados, garantindo sua efetividade. A periodicidade deve ao menos ser uma por ano, a ser determinada pelo Comitê de Segurança, considerando o nível de risco do negócio. Devem ser mantidas evidências do sucesso dos testes feitos.

5.11 Pirataria

Este item se destina a todos os usuários e administradores de servidores de redes ou computadores, inclusive portáteis, conectados ou não a uma rede e tem como objetivo garantir que sejam tomadas medidas adequadas para coibir a pirataria de softwares dentro das instalações das empresas do BB.

i. Normas contra pirataria:

A quantidade de licenças de softwares não pode ser inferior à quantidade de softwares instalados, mesmo que para fins de testes ou treinamentos, a não ser que esta situação esteja coberta contratualmente.

Não é permitido duplicar software de propriedade do BB a não ser com a finalidade de cópia de segurança e mesmo assim, somente por pessoas autorizadas. Uma licença de uso de software do BB só pode ser instalada em computadores do BB.

Todo software de demonstração deve vir acompanhado de uma autorização formal da empresa proprietária, indicando onde pode ser instalado e por quanto tempo.

É proibida a utilização e reprodução não autorizada de manuais, livros, revistas, periódicos protegidos por direitos autorais.

ii. Responsabilidades quanto à pirataria:

- Verificar se o software a ser instalado é original, conferindo o mesmo com as devidas licenças de uso;
- Se a instalação foi autorizada pelo Responsável Administrativo da Unidade, verificar se o software foi previamente homologado pela equipe técnica; e
- Implementar mecanismos que dificultem a pirataria através de qualquer meio.

5.12 Utilização Segura de Hardware e Software

Todos os equipamentos portáteis (notebooks, laptops, netbooks, ultrabooks, tablets e smartphones) que tenham capacidade de armazenamento de dados, devem seguir os princípios de segurança contidos nesta política. Quando estes equipamentos contiverem informações que não possam ser de conhecimento público, os dados devem ser criptografados ou ter seu acesso protegido por senha.

É proibida a utilização de qualquer equipamento particular na rede corporativa do Banco do Brasil.

É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de "softwares" ou de quaisquer programas e produtos, mesmo aqueles desenvolvidos pelas áreas técnicas ou por terceiros.

5.13 Acesso à Internet

A Internet abrange vários aspectos e serviços (websites de serviços governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades de negócio. A restrição a websites não relativos aos negócios da organização deve ser implementada, garantindo o uso efetivo da rede de Internet.

O acesso à Internet deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia (Nome do usuário e endereço acessado são informações obrigatórias no rastreamento).

O usuário deve restringir o acesso aos websites ainda não bloqueados que possam manchar a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não têm relação com os objetivos de negócio da organização (Webmail, jogos etc.). Deve também comunicar o endereço eletrônico desses websites à área de Segurança da Informação, que deverá realizar seu imediato bloqueio.

O acesso à Internet deve ser feito através de "Servidores de Acesso" protegidos por sistemas de Firewall. Quando for necessário o acesso utilizando uma

segunda conexão através de modem ou rede wi-fi, a configuração da máquina deve garantir o isolamento da rede normal de serviço da empresa, evitando assim que uma contaminação seja propagada. Os requisitos de segurança destas máquinas em particular devem ser respeitados (antivírus e firewall local). Casos específicos como esses devem ser aprovados pelos responsáveis da área de Segurança da Informação.

5.14 Acesso ao Correio Eletrônico

O BB disponibiliza aos seus colaboradores a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outros grupos que tenham relação comercial. É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios.

As mensagens de correio eletrônico devem ser rastreadas, a fim de permitir o monitoramento para identificar o uso indevido da tecnologia.

6. Plano de continuidade do negócio

Um plano de continuidade do negócio deve garantir a recuperação dos processos críticos do BB quando da indisponibilidade do ambiente ou de quaisquer recursos que impossibilitem o desenvolvimento ou as operações das áreas de negócio.

É de responsabilidade de cada área envolvida no desenvolvimento dos negócios, elaborar, testar e implantar seus planos de contingência. Adicionalmente, o plano deve ser revisado e atualizado anualmente.

A definição de processos críticos de uma empresa ou área, obrigatoriamente, deve obedecer a critérios emanados pelos Diretores responsáveis pela instituição / área.

i. Pontos a serem observados no plano de continuidade do negócio:

Na elaboração de um plano de continuidade do negócio os pontos abaixo devem ser observados:

- As funções críticas devem ser identificadas e definidas;
- Traçar uma estratégia para recuperação de cada função crítica;
- Priorizar as funções críticas para ordenar sua recuperação;
- Identificar as atividades necessárias para recuperar cada função;
- Quantificar os recursos humanos e técnicos necessários ao cumprimento do plano;
- Documentar os processos críticos;
- Identificar os responsáveis pela recuperação de cada processo ou função;
- Ações para restabelecer a operação normal; e
- Identificar os recursos de backup (infraestrutura, hardware, software, sistemas aplicativos e telecomunicações).

ii. Revisões periódicas do plano de continuidade do negócio:

O plano de continuidade do negócio deverá sofrer revisões anuais a fim de identificar pontos que estiverem em desacordo com a situação atual. Deverão ser observados os pontos abaixo:

- Troca de fornecedores ou contratados;
- Alteração de endereços ou números de telefones;
- Mudanças nas prioridades de recuperação;
- Interdependência entre sistemas e aplicativos;
- Mudanças nas funções e nos processos críticos de negócio;
- Mudanças nas práticas operacionais; e
- Atualização da relação de colaboradores críticos.

7. Plano de Conscientização de Segurança da Informação

Um plano de conscientização da segurança da informação deve ser elaborado e executado para atingir o seguinte objetivo:

"Garantir que a Segurança da Informação não seja apenas conhecida, mas compreendida por todos os colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de Segurança de forma a atingir uma melhor utilização e proteção à informação.".

As diretrizes básicas são:

- Elaboração de um processo de treinamento continuado contemplando todos os níveis funcionais do BB;
- Divulgação de diversos materiais e alertas referente a Segurança da Informação para colaboradores e clientes;
- Criação de procedimentos de aferição do nível de conhecimento dos usuários em geral;
- Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral; e
- Revisão periódica do plano, adequando as ações às novas necessidades, evitando torná-lo repetitivo.

8. Canais de Relacionamento com o Cliente

Os seguintes canais eletrônicos de relacionamento devem garantir a positivação de informações do cliente:

• Internet Banking e Aplicativo Móvel: através de CPF, senha de acesso e chave se segurança ou confirmação de informações de conhecimento pessoal do cliente.

• SAC: através de CPF e confirmação de informações de conhecimento pessoal do cliente.

• WhatsApp (corporativo): validação do número de telefone que originou a comunicação e confirmação de informações de conhecimento pessoal do cliente.

Observação: Esse canal não é utilizado para serviços transacionais e tem uso permitido apenas através de plataforma corporativa que possui controles de segurança.

Na utilização de mensagens de correio, a privacidade da informação deve ser preservada e a mensagem criptografada. Deve-se utilizar certificados que garantam a integridade da mensagem ou senhas em arquivos que devem ser transmitidas ao cliente por outro meio de comunicação.

Os canais de relacionamento também devem oferecer conteúdo educativo sobre precauções e cuidados a respeito de aspectos de segurança a fim de proteger acessos, contas e recursos dos clientes com o Banco do Brasil.

9. Plano de Resposta a Incidentes

É de responsabilidade da Unidade de Segurança Digital e da Informação – USD, publicar e revisar o plano de resposta a incidentes cibernéticos, esse plano deve conter cada etapa de cada tratativa a partir da identificação de um incidente. Seu objetivo é criar uma abordagem e conduta, minimamente necessária, em caso de um incidente cibernético na instituição.

Anexo III – Código de Ética

Código de Ética do Banco do Brasil 2023 – 2024

Propósito: “Ser próximo e relevante na vida das pessoas em todos os momentos.”

Valores:

- Proximidade: Somos presentes e proativos para encantar nossos clientes.
- Inovação: Inovamos para simplificar as soluções e facilitar a vida das pessoas.
- Integridade: Somos confiáveis, éticos e transparentes.
- Eficiência: Otimizamos os recursos disponíveis para criar valor aos nossos públicos de relacionamento.
- Compromisso com a sociedade: Consideramos o interesse coletivo na tomada de nossas decisões.

O código de ética é aplicado à:

- Alta administração: Conselheiros, Presidente, Vice-Presidentes e Diretores, inclusive de empresas controladas.
- Funcionários: lotados no Brasil e no exterior.
- Colaboradores: Estagiários, aprendizes, dirigentes e empregados de empresas contratadas.
- Demais: àqueles que estejam atuando ou prestando serviços em nome do Banco do Brasil ou para o Banco do Brasil.

Princípios do Código de Ética:

- Honestidade: O Banco espera que a conduta de seus funcionários tenha como padrão a honestidade. Devemos fazer somente aquilo que é correto, devemos agir de boa-fé, com integridade e sinceridade nos assuntos que afetam deveres e interesses do Banco.
- Responsabilidade: Cada membro do Banco é responsável por suas ações e decisões. Devemos, independentemente da posição que ocupamos, ser responsáveis pela criação de um ambiente transparente, respeitoso e seguro, a fim de que os negócios sejam éticos

e sustentáveis. Também é nossa responsabilidade zelar para que atos irregulares não ocorram no Banco.

- Transparência: O Banco zela pela transparência de suas ações. As informações devem ser completas, precisas e claras. A confiança de nossos parceiros está ligada ao livre acesso que o Banco dá às informações de seus relatórios, prestações de contas e tomadas de decisão. O sigilo e a confidencialidade das informações permeiam e são exigidos em nossas ações no Banco. Entretanto, ações executadas deliberadamente às escondidas não são éticas.
- Respeito: O Banco do Brasil não tolera desrespeito à dignidade, à igualdade, à diversidade e à privacidade das pessoas. O ambiente de trabalho deve ser um local de profissionalismo, em que se respeitam as diferentes culturas e compreensões de mundo e onde o respeito às leis e aos regulamentos internos do BB são prioridade.

1. Respeito

1.1 Respeitamos a diversidade das pessoas que formam o ambiente de trabalho e que mantêm relacionamento com o Banco do Brasil.

1.2 Encorajamos a cultura de respeito e repudiamos a violência.

1.3 Devemos zelar pelo estabelecimento de um ambiente de trabalho digno e saudável, pautando as relações pelo respeito e cordialidade, independentemente da posição exercida na organização.

1.4 Devemos pautar nossas relações pelo respeito às diferenças, sendo elas físicas, raciais, culturais, religiosas, de orientação sexual, sociais, linguístico regionais, etárias, de ideias, de origem, de capacidade, de aparência, de classe, de estado civil ou de identidade de gênero.

1.5 Devemos respeitar as normas sociais e culturais da comunidade em que atuamos, apresentando e nos comportando de maneira adequada e alinhada à posição exercida.

1.6 Devemos prevenir constrangimentos e prejuízos à imagem do Banco e de seus funcionários.

1.7 Desautorizamos que se inicie ou divulgue, em qualquer meio - interno ou externo - críticas ofensivas à honra ou calúnias que exponham a imagem do BB ou de quaisquer de nossas áreas ou funcionários.

2. Boas práticas de relacionamento

2.1 Primamos pela confiança, honestidade e ética em nossas práticas comerciais, atuando de forma transparente, imparcial e íntegra.

2.2 Devemos oferecer produtos e serviços, bem como, prestar atendimento com honestidade, diligência e ética.

2.3 Devemos nos comprometer com o bom clima de trabalho, pautando nossas condutas pelo respeito e tolerância.

2.4 Devemos manter a comunicação respeitosa e profissional com nossos pares, gestores, subordinados, clientes internos e externos. Ambiente de Trabalho Presencial, Remoto ou Contingencial

2.5 Desautorizamos a emissão ou reprodução de comentários que possam prejudicar a convivência harmoniosa no ambiente de trabalho.

2.6 Devemos desenvolver atividades com responsabilidade, autonomia e comprometimento.

2.7 Devemos realizar as atividades que nos são confiadas, assumindo a responsabilidade pela tarefa.

2.8 Devemos acompanhar e conduzir, com tempestividade e comprometimento, as demandas encaminhadas através das ferramentas oficiais de comunicação interna do Banco.

2.9 Devemos desenvolver nosso trabalho diário observando as orientações de segurança.

2.10 Consideramos a segurança e a saúde no trabalho pilares institucionais.

2.11 Devemos cumprir as normas de segurança e saúde do trabalho.

2.12 Proibimos que se trabalhe embriagado e/ou sob efeito de drogas ilícitas.

2.13 Devemos contribuir, nas nossas atividades diárias, para a manutenção do caráter laico e apartidário da Empresa.

2.14 Repudiamos condutas que possam caracterizar assédio de qualquer natureza.

2.15 Repudiamos condutas que possam caracterizar discriminação ou sua indução; coação, perseguição ou constrangimento; desrespeito às atribuições funcionais; desqualificação pública, ofensa ou ameaça.

2.16 Orientamos que funcionários mantenham situação econômico-financeira compatível com a ocupação e a renda comprovadas.

2.17 Devemos supervisionar e adotar medidas inibidoras de irregularidades.

Boas práticas de relacionamento - Líderes:

2.18 Esperamos que nossos líderes promovam o desenvolvimento e inspirem suas equipes, estimulando o engajamento e buscando formar sucessores para desafios atuais e futuros.
2.19 Exigimos que os nossos líderes respeitem o Código de Ética e a Política de Relacionamento com Clientes e Usuários, promovendo a indução de seus liderados para esse mesmo fim.
2.20 Esperamos que os nossos líderes construam uma relação sólida com os clientes, fornecendo soluções adequadas para eles.
2.21 Esperamos que nossos líderes atuem com visão e propósito, apresentando a estratégia do BB de uma perspectiva assertiva para obter o apoio e o comprometimento dos liderados.
2.22 Exigimos que os nossos líderes sejam éticos, referência de postura adequada e incentivadores do trabalho em equipe como prática de colaboração e de compartilhamento de conhecimentos e experiências.
2.23 Determinamos que a comunicação dos nossos líderes esteja alinhada à estratégia do Banco, buscando o equilíbrio entre pessoas, processos e resultados, demonstrando cuidado com clientes, funcionários, sociedade e acionistas.
2.24 Esperamos dos nossos líderes coragem para ousar e que desenvolvam adaptabilidade, resiliência e sabedoria frente a circunstâncias desafiadoras, fazendo constantemente a gestão dos riscos.
2.25 Recomendamos que os nossos líderes tenham empatia, controle emocional e respeito à individualidade dos liderados.
2.26 Esperamos que nossos líderes sejam promotores do diálogo com respeito, boa educação e assertividade, colocando em prática a Comunicação Não Violenta e a escuta ativa.
2.27 Esperamos que os nossos líderes contribuam para o desenvolvimento dos liderados, incentivando a autonomia, a inovação e a transformação cultural.
2.28 Desejamos que os nossos líderes valorizem vitórias e conquistas da equipe como incentivo à continuidade dos bons resultados.
2.29 Esperamos dos nossos líderes conhecimento de processos mais eficazes e eficientes, antecipando e adotando iniciativas inovadoras no desenvolvimento de soluções digitais para obter resultados consistentes.
2.30 Esperamos dos nossos líderes, além da conduta ética, a disseminação dos valores da organização e preceitos do Código de Ética, contribuindo para a aplicação deste documento.

Boas práticas de relacionamento - Liderados:

2.31 Exigimos que os nossos liderados respeitem o Código de Ética e a Política de Relacionamento com Clientes e Usuários.
2.32 Esperamos que os nossos liderados tenham respeito, tolerância, controle emocional e maturidade, colocando em prática a Comunicação Não Violenta e a escuta ativa.
2.33 Esperamos que os nossos liderados sejam protagonistas da sua carreira e promovam seu autodesenvolvimento, demonstrando iniciativa e comprometimento, além de capacidade de adaptação a mudanças de cenário.
2.34 Esperamos dos nossos liderados a parceria com a gestão, com foco nas boas práticas de relacionamento e na condução dos processos.
2.35 Esperamos que os nossos liderados desenvolvam o pensamento estratégico, a destreza digital, a leitura de cenário, a criatividade e inovação.

Boas práticas de relacionamento – Parceiros e Clientes:

2.36 Orientamos parcerias com agentes que assegurem valores como: integridade, ética, idoneidade e respeito à comunidade e ao meio ambiente.
2.37 Exigimos que os impactos socioambientais sejam medidos e considerados na realização de parcerias, convênios, protocolos de intenções e de cooperação técnico-financeira com entidades externas privadas ou públicas.
2.38 Orientamos que contatos e negócios com clientes sejam pautados pelo respeito, idoneidade e profissionalismo e que os produtos e serviços oferecidos sejam adequados ao perfil dos clientes e de acordo com a legislação.
2.39 Orientamos que entidades ligadas ao Banco do Brasil pautem seus direcionamentos estratégicos e de negócios por princípios éticos.
2.40 Proibimos a utilização de subterfúgios para o atingimento de metas, a exemplo dos negócios não sustentáveis e burla dos sistemas e regras da corporação.
2.41 Respeitamos a liberdade de associação sindical e buscamos conciliar, de forma transparente, interesses da empresa com interesses de funcionários e de nossas entidades representativas tendo a negociação como prática permanente.

Boas práticas de relacionamento – Fornecedores:

2.42 Devemos conduzir processos de licitação, contratação e formalização de acordos, convênios e parcerias com lisura, ética, integridade e imparcialidade.
2.43 Devemos adotar ações e procedimentos para prevenir fraudes e ilícitos nos processos licitatórios, na execução e acompanhamento de contratos administrativos ou em interação com o setor público.
2.44 Orientamos que critérios de seleção, contratação e avaliação devem ser determinados de forma imparcial e transparente, permitindo pluralidade e concorrência entre fornecedores.
2.45 Devemos exigir de fornecedores: cumprimento da legislação trabalhista, previdenciária e fiscal; cumprimento da legislação e das regulamentações relativas à prevenção e ao combate à corrupção; não utilização de trabalho infantil ou escravo; adoção de boas práticas de preservação ambiental; não adoção de atos de corrupção contra governos e a administração pública brasileira ou estrangeira.
2.46 Orientamos os fornecedores a seguir as diretrizes deste Código de Ética.

Boas práticas de relacionamento – Acionistas, investidores e credores:

2.47 Somos transparentes e ágeis no fornecimento de informações, observando regras de sigilo e confidencialidade.
2.48 Elaboramos demonstrações financeiras em conformidade com a lei, princípios e normas de contabilidade para representar adequadamente o resultado das operações, os fluxos de caixa e a posição patrimonial e financeira da Empresa.

Boas práticas de relacionamento – Concorrentes:

2.49 Definimos que a ética, a integridade e a civilidade devem ser princípios norteadores das nossas relações com a concorrência. Trocas de informações só podem ocorrer de maneira lícita, transparente e fidedigna, preservando os princípios do sigilo bancário e os interesses da Empresa.
2.50 Desaprovamos a emissão de juízo de valor sobre a concorrência ou a depreciação de seus produtos e serviços.
2.51 Proibimos práticas inadequadas na oferta de produtos e serviços, inclusive a imposição na efetivação de negócios.

Boas práticas de relacionamento – Governos:

2.52 Somos parceiros do setor público na implementação de políticas e projetos públicos e programas de governo voltados para o desenvolvimento social e econômico do Brasil e dos países em que atuamos, com foco na sustentabilidade.
2.53 Articulamos a convergência de interesses e necessidades do Setor Público com o Setor Privado e segmentos socioeconômicos das sociedades com as quais nos relacionamos.
2.54 Devemos atuar nas relações com o poder público em conformidade com diretrizes internacionais no que diz respeito prevenção e combate à evasão fiscal, à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo.
2.55 Repudiamos atos de corrupção praticados contra o Setor Público e a administração pública brasileira ou estrangeira, a exemplo de: garantir, prometer, oferecer ou dar, direta ou indiretamente, qualquer vantagem indevida a agente público ou a terceiro a ele relacionado; financiar, custear, patrocinar ou de qualquer modo subvencionar prática de ato ilícito; induzir a realizar ou deixar de realizar ação em violação às obrigações legais; obter, manter ou direcionar negócios de maneira indevida; praticar sonegação de impostos, evasão de divisas e demais crimes fiscais; afetar ou influenciar ato ou decisão; utilizar intermediário - pessoa física ou jurídica - para ocultar ou dissimular interesse ou identidade de beneficiários de atos praticados; impedir, perturbar ou manipular o caráter competitivo das compras públicas e processos licitatórios; dificultar ou intervir na atividade de investigação ou fiscalização.
2.56 Devemos estabelecer independentemente de convicções ideológicas individuais, relacionamento cortês com o Setor Público brasileiro e com o poder público dos países em que atuamos.
2.57 Proibimos o financiamento de partidos políticos ou candidatos a cargos públicos no Brasil e nos países em que atuamos em nome do Banco, ou de seus representantes.
2.58 Proibimos dar, oferecer, prometer ou autorizar que se dê qualquer coisa de valor a funcionário do governo brasileiro ou estrangeiro, diretamente ou por meio de intermediário, a fim de influenciar ação para obter vantagem indevida.

3. Necessidade da obediência ao que é legal

3.1 Pautamos nossa atuação pelos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

3.2 Repudiamos práticas ilícitas, principalmente fraude, suborno, extorsão, corrupção, nepotismo, propina, agiotagem, lavagem de dinheiro, evasão de divisas e financiamento do terrorismo.

Necessidade da obediência ao que é legal – Conformidade:

3.3 Ratificamos a necessidade de todos os funcionários e os membros da alta administração possuírem conhecimentos sobre as Políticas do Banco, a legislação e a regulamentação em vigor inerentes às suas atividades.

3.4 Devemos atuar em conformidade com os normativos internos, as leis e normas de ordenamento jurídico brasileiro e dos países onde atuamos.

3.5 Vedamos o relacionamento negocial com pessoas e organizações envolvidas em atividades ilícitas.

3.6 Desautorizamos a prática de ato que possa acarretar ação cível ou trabalhista ou que cause prejuízo ao Banco.

3.7 Proibimos a formalização de decisões relativas a operações sem prévia e formal autorização do cliente.

3.8 Proibimos a comercialização e o consumo de drogas ilícitas no ambiente de trabalho.

3.9 Devemos atender às solicitações de órgãos externos de regulamentação e fiscalização e de auditorias externa e interna nos prazos estabelecidos.

3.10 Devemos assegurar informação legítima, íntegra, objetiva, atual e clara em divulgações públicas, relatórios e documentos disponibilizados aos órgãos reguladores de países onde atuamos.

3.11 Orientamos os funcionários e os membros da alta administração a realizarem anualmente capacitação sobre ética disseminando os preceitos contidos neste Código e na Trilha da Ética e sobre as Políticas associadas à gestão de riscos, em especial ao Risco de Conduta.

3.12 Orientamos os funcionários, estagiários e aprendizes a registrar ciência do Código de Ética do BB a cada campanha de leitura.

Necessidade da obediência ao que é legal – Alta Administração:

3.13 Orientamos a Alta Administração a observar normas jurídicas que lhe são aplicáveis no exercício da função, inclusive as de direito público.

3.14 Orientamos os Estatutários a seguir, além deste Código de Ética, o Código de Conduta da Alta Administração Federal, que dispõe, entre outros assuntos, sobre: conflito de interesses; sigilo e comunicação de informações relevantes obtidas em razão da função ocupada; quarentena estatutária.

4. Conflito de interesses

4.1 Compreendemos que há conflito quando um funcionário tem interesses privados que influenciam no desempenho de seus deveres e responsabilidades no Banco.

4.2 Entendemos que a forma correta de evitar o conflito de interesses é buscando a imparcialidade. Agir de forma imparcial significa, por vezes, declarar-se impedido de realizar determinadas atividades.

4.3 Devemos exercer nossa atividade de forma isenta, eximindo-nos de usar a condição de funcionário para obter vantagens para nós ou para terceiros. É dever de cada um evitar a ocorrência de conflito de interesses.

4.4 Devemos comunicar, de forma imediata, casos de conflito de interesses ou presunção de sua existência ao superior hierárquico ou à Ouvidoria Interna.

4.5 Devemos apoiar e participar de estratégias do BB e de seus gestores de risco visando prevenir e mitigar a ocorrência de conflito de interesses.

4.6 Advertimos que as ações exemplificadas a seguir configuram conflito de interesses:

• Deliberar sobre assuntos de interesse conflitante com o do Banco.

• Celebrar contrato administrativo ou celebrar contrato em nome do Banco, excetuada contratação de operações bancárias, desde que observados os limites dispostos nos termos da legislação, regulamentações aplicáveis bem como nas Políticas Especificas de Transações com Partes Relacionadas (TPR) e Políticas de Credito do Banco, com pessoa que tenha relação de parentesco até o terceiro grau com: a) dirigente do BB; b) empregado do BB cujas atribuições envolvam atuação na área responsável pela licitação ou contratação; c) autoridade de ente público a que o BB está vinculado.

• Manter sob subordinação hierárquica direta cônjuge, companheiro(a) ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o 3º grau.

• Conduzir assuntos ou negócios com agente público com poder decisório no âmbito dos órgãos e entidades do governo com o qual tenha relação de parentesco, em linha reta ou colateral, por consanguinidade ou afinidade, até 3º grau.

• Permitir que atividades internas extrapolem o ambiente restrito, afetando interesses do Banco.

• Utilizar a condição de funcionário para obter empréstimo pecuniário de cliente, fornecedor ou prestador de serviços.

• Utilizar informação privilegiada sobre ato ou fato relevante ainda não divulgado no mercado a que tenha tido acesso em razão de cargo ou função.

• Utilizar informação interna para realizar negócios pessoais com terceiros, como clientes, fornecedores, prestadores de serviços, parceiros de negócios, correspondentes, etc.

• Utilizar o nome do Banco do Brasil no exercício de seus direitos políticos.

• Conduzir carreira no Banco recorrendo à intermediação de terceiros.

• Usar de sua posição e poder para nomear, contratar ou favorecer um ou mais parentes em detrimento de pessoas e empresas com perfil e competências mais adequados, configurando prática de nepotismo.

• Desempenhar atividades externas que possam constituir prejuízo ou concorrência para o Banco.

4.7 Vedamos a realização de Transações com Partes Relacionadas (TPR) em condições diversas às de mercado.

• Em função das atividades desenvolvidas no BB, um funcionário obtém informações de determinada empresa listada em bolsa de valores. Ciente da valorização de seus papéis, adquire elevada quantidade, a fim de lucrar com o movimento.

5. Tomada de Decisão

5.1 Todas as vezes que você for tomar uma decisão, faça as seguintes perguntas, para avaliar se ela está adequada:

A sua decisão atende aos interesses do Banco?

Essa decisão pode ser justificada aos seus colegas e superiores?

Excetuando situações em que há a necessidade de sigilo e confidencialidade, sua decisão pode ser pública?

Se você responder NÃO para alguma dessas perguntas, então PARE e procure ajuda.

6. Presentes, brindes, hospitalidade e favores

6.1 As regras a seguir referem-se ao relacionamento do Banco do Brasil com terceiros, como cliente, fornecedor, prestador de serviço, parceiro de negócios, correspondente, etc.
6.2 Vedamos o recebimento pelo funcionário do BB de qualquer valor em espécie como benefício próprio.
6.3 Proibimos o recebimento e solicitação de benefício ou remuneração em retorno por serviço prestado na realização de nossas atividades na qualidade de funcionários do BB.
6.4 Desaprovamos o recebimento ou a oferta de presentes ou brindes que comprometam a percepção de profissionalismo e de imparcialidade da empresa, independentemente do valor.
6.5 Autorizamos aceitar presente ou brinde avaliado em até R$390,00, que se refere a 1% do teto remuneratório previsto no inciso XI do caput do art. 37 da Constituição Federal, desde que não caracterize manipulação de processos decisórios ou obtenção de vantagens indevidas.
6.6 Orientamos a doação à Fundação Banco do Brasil ou à instituição beneficente sem fins lucrativos presentes recebidos, caso tenha sido inviável a recusa ou a devolução imediata. A doação deve ser comunicada no Portal Pessoas (dipes.bb.com.br) > Crachá > Você > Atuação > Presentes/Brindes > Incluir Novo Item.
6.7 Orientamos que, para oferecer brindes e presentes em nome do BB para agente público, sejam observados os limites previstos na Constituição e na legislação local, bem como na legislação que trata de suborno transnacional e nas regras e políticas da instituição, ente ou órgão público daquele que a receberá.
6.8 Autorizamos aceitar hospitalidade, desde que autorizado no âmbito do órgão, entidade, diretoria ou unidade BB, de acordo com os critérios legais e desde que não haja comprometimento das premissas de imparcialidade e moralidade.

7. Bens e recursos do Banco do Brasil

7.1 Proibimos o uso de recursos físicos, tecnológicos, bens e serviços exclusivos ao desempenho de nossas atribuições, para fins particulares.
7.2 Devemos nos limitar a instalar, usar ou permitir o uso de programa de computador (software) licenciados ou autorizados.
7.3 Devemos preservar a identidade institucional, evitando usar o nome da Empresa, suas marcas e símbolos sem necessidade relevante e justificada ou sem autorização, sobretudo no relacionamento com público externo e nas exposições em redes sociais.

7.4 Devemos observar a competência restrita dos porta vozes para atender demanda de informações pela mídia, de forma alinhada com a estratégia corporativa do BB, respeitando visão, propósito e valores da Empresa.
7.5 Proibimos o uso de instalações, equipamentos, materiais de trabalho e rede eletrônica de comunicações para assuntos político-partidários, religiosos ou de interesse comercial próprio ou de terceiros.
7.6 Devemos zelar pelo patrimônio e imagem do BB e disseminar este cuidado.
7.7 O BB zela por coerência e uniformidade das informações prestadas pelas pessoas autorizadas a falar em nome do Banco do Brasil ao público em geral e com a imprensa. Transparência, simplicidade e agilidade na prestação de informações em nome do BB estão entre os principais princípios de atuação do BB junto à mídia.

8. Propriedade intelectual e propriedade da informação

8.1 Preservamos a segurança da informação, pois a informação corporativa é um ativo e possui valor para a Organização.
8.2 Devemos nos limitar a instalar, usar ou permitir o uso de programa de computador (software) licenciados ou autorizados.
8.3 Devemos observar normas da propriedade intelectual de livros, textos, imagens e outros produtos protegidos por direito autoral.
8.4 Devemos observar diretrizes e políticas de segurança da informação do BB, atentando-nos para a criticidade das informações.
8.5 Proibimos que funcionários tratem de assuntos sigilosos e de uso interno em salas de conversação, redes sociais e aplicativos com acesso pela internet não autorizados pelo Banco.
8.6 Devemos proteger informações de propriedade do Banco do Brasil como forma de garantir integridade, confidencialidade e disponibilidade. não poderão ser divulgados sem prévia autorização estudos, metodologias, técnicas, materiais ou modelos desenvolvidos para o banco.
8.7 Devemos consultar o cadastro e as informações de produtos e serviços de funcionários e correntistas apenas por necessidade do serviço, preservando o sigilo cadastral, bancário, empresarial e profissional.
8.8 Devemos resguardar o sigilo de informação do Banco do Brasil, relativo a ato ou fato relevante aos quais tenhamos acesso privilegiado em razão da posição ou função que ocupamos.

Ética

8.9 Devemos prestar esclarecimentos fidedignos e tempestivos quando solicitados pelo Banco, mesmo quando estivermos em situação de disponibilidade para outra empresa ou cedidos para órgão externo.
8.10 Devemos assegurar que registros contábeis e demonstrações financeiras sejam verdadeiros, completos, precisos, claros e estejam em conformidade com a legislação, com os princípios e com as normas de contabilidade e controles internos.

Uso ético dos dados

8.11 Tratamos de maneira responsável e ética os dados internos e externos coletados, de acordo com a legislação, durante todo o ciclo de vida da informação.
8.12 Devemos fazer gestão das informações que nos são confiadas e remetidas pelos diversos canais corporativos de comunicação interna.
8.13 Utilizamos mecanismos de segurança para proteção de dados e informações de clientes, fornecedores, parceiros e demais intervenientes.
8.14 Devemos realizar nossas atividades respeitando a privacidade do cliente e a legislação relativa ao assunto, inclusive no uso e tratamento de bases de dados analíticas.
8.15 O BB tem um compromisso com a ética e a integridade em sua atuação e no manejo de informações sob sua guarda. A postura ética deve se dar em qualquer ambiente, inclusive por meio das novas formas de interação, como o metaverso, e na análise de dados, com o uso da a inteligência artificial.

9. Envolvimento com a comunidade e sustentabilidade

9.1 Adotamos a responsabilidade social, ambiental e climática na definição de políticas, normas e procedimentos de prevenção e combate à corrupção, bem como à lavagem de dinheiro e ao financiamento do terrorismo.
9.2 Estimulamos ações empreendedoras com parceiros que abordam proativamente impactos sociais, ambientais e climáticos.
9.3 Repudiamos o trabalho degradante: infantil, forçado e escravo.

9.4 Valorizamos vínculos estabelecidos com as comunidades nas quais atuamos e respeitamos seus valores culturais pois reconhecemos a necessidade de retribuir à comunidade parcela do valor agregado aos negócios.
9.5 Apoiamos iniciativas de desenvolvimento sustentável e participamos de empreendimentos voltados à melhoria das condições sociais da população.

10. Uso responsável das mídias digitais

10.1 Entendemos que a comunicação interna deve contribuir para o fortalecimento da relação entre a Empresa e os funcionários.
10.2 Primamos pela comunicação inclusiva e que cria condições favoráveis à ação negocial e à realização do trabalho, com foco na transparência, clareza e objetividade.
10.3 Devemos usar de forma responsável as mídias digitais e aplicar boas práticas de comunicação alinhadas aos princípios de integridade, transparência e respeito.

Protagonismo e debate colaborativo

10.4 Valorizamos manifestações no ambiente digital que respeitem a diversidade de ideias e o posicionamento da Empresa.
10.5 Proibimos a vinculação do Banco do Brasil a comentários e postagens de informações ou imagens ofensivas e/ou que violem a privacidade de funcionários e terceiros em mídias digitais e redes sociais.
10.6 Proibimos a emissão ou compartilhamento de informações de caráter discriminatório ou ofensivo que exponha a imagem do Banco, de seus funcionários e do Conglomerado.

11. Dúvidas e denúncias

Denúncias devem ser encaminhadas à Ouvidoria Interna e/ou o Canal de Denúncias, mesmo de forma anônima. O sigilo da fonte e a confidencialidade das informações são premissas dos canais internos.

Prioritariamente, denúncias que tratam de ilícitos e demais irregularidades devem ser remetidas ao Canal de Denúncias. Denúncias que envolvem comportamento e relacionamento interpessoal são acolhidas pela Ouvidoria Interna BB.

11.1 Valorizamos sua manifestação. Se perceber algo que fira o Código de Ética do Banco do Brasil, é seu dever denunciar. O BB possui dispositivos para promover a proteção ao denunciante de boa-fé, podendo, inclusive, adotar medidas administrativas julgadas pertinentes.
11.2 Repudiamos qualquer tipo de retaliação ao autor de denúncias, ou àqueles que contribuam de alguma forma para o esclarecimento dos fatos. Casos desta natureza serão avaliados sob aspecto ético e podem ser encaminhados para tratamento disciplinar. O denunciante que vivenciar situação de coação, perseguição ou retaliação deve acionar o canal da Ouvidoria Interna, relatando o fato ocorrido.
11.3 Entendemos que o descumprimento das diretrizes deste Código de Ética representa grave manifestação contra a ética e contra princípios administrativos do Banco do Brasil.
11.4 Para comunicar à Diretoria de Controles Internos-Dicoi/ DF indício de ilícitos ou irregularidades, por meio do Canal de Denúncias do Banco do Brasil, acesse o Portal BB (www.bb.com.br/canaldedenunciasbb).
11.5 Recomendamos que, em caso de dúvida quanto ao exercício de atividade laboral remunerada ou não, paralela ao Banco, o funcionário encaminhe consulta por meio do Sistema Eletrônico de Prevenção de Conflito de Interesses (SeCI), disponível no site da Controladoria-Geral da União - CGU.
11.6 Sugerimos que, em caso de dúvida quanto à aplicação do Código de Ética, converse com seu gestor ou consulte o Comitê Estadual de Ética, por meio de registro no Portal da Ouvidoria Interna, na intranet.

12. Carta de Encerramento

Este Código de Ética foi elaborado pela Diretoria Gestão da Cultura e de Pessoas com a participação de vários colegas, validado por todas as Unidades Estratégicas do BB, pelo Comitê Executivo Pessoas e Cultura Organizacional, Conselho Diretor e Conselho de Administração do BB. Essa construção colaborativa retrata que a ética faz parte da cultura do Banco do Brasil.

O documento deve ser revisado a cada três anos ou, extraordinariamente, a qualquer tempo. A Diretoria Gestão da Cultura e de Pessoas é a área responsável pela estruturação, atualização, disseminação e implementação deste Código.

Para facilitar seu entendimento, utilizou-se linguagem simples e clara. Exemplos, perguntas e respostas foram construídos com o objetivo de ilustrar a aplicação da ética no dia a dia de trabalho.

Além de ser um instrumento que orienta os funcionários na tomada de decisões, o Código de Ética apresenta condutas esperadas pelo BB e as que são expressamente vedadas, indicando, de forma objetiva e prática, as responsabilidades dos colaboradores, inclusive da Alta Administração, a fim de contribuir para credibilidade, idoneidade e perenidade de nossa Organização.

Os pressupostos e orientações constantes no Código de Ética do Banco do Brasil devem ser observados com atenção, cuidado e visão de protagonismo, pois a responsabilidade pela aplicação e disseminação é de todos nós.

Afinal, ética e integridade são a base da confiança.

Código de Ética - Banco do Brasil (2023-2024) adaptado de https://www.bb.com.br/docs/portal/dipes/Codigo_de_Etica.pdf?pk_vid=f9c9b1f4ca08e2c11712926044dfe0ed