Declaração de Apetite por Riscos

SUMÁRIO

1. INTRODUÇÃO E OBJETIVO

Em atendimento às exigências do Banco Central do Brasil ("BACEN"), por meio da Resolução nº 4.557/17, do Conselho Monetário Nacional ("CMN", a "Resolução 4.557") e aderência as melhores práticas do mercado, o Conglomerado Prudencial XP ("XP") estabelece, por meio desta Declaração de Apetite a Riscos ("RAS" – *Risk Appetite Statement*), os tipos de riscos e as respectivas tolerâncias que está disposta a assumir no cumprimento de seus objetivos e os processos existentes para gerenciamento deles de forma efetiva e prudente.

A RAS, em conjunto com a Política de Gestão Integrada de Riscos, contribui com o compromisso da XP de manter os mais altos padrões de governança e conformidade, consistentes com a manutenção da credibilidade de seus clientes e stakeholders e, principalmente, com o pleno cumprimento de suas obrigações regulamentares, abrangendo as exigências da Resolução 4.557.

As definições, premissas e regras formalizadas nestas RAS se aplicam ao Conglomerado Prudencial XP, incluindo os prestadores de serviços relacionados diretamente com as atividades dos negócios em território nacional.

O gerenciamento de riscos está no cerne das decisões estratégicas da XP com envolvimento direto da Diretoria. A XP trabalha, constantemente, para fortalecer a cultura e processos de gerenciamento de riscos, a fim de mitigar os efeitos do aumento da volatilidade no ambiente de negócios e da complexidade regulatória, de forma a garantir o crescimento seguro dos seus negócios.

Por meio da utilização de modernas ferramentas de gerenciamento de riscos, melhorias nos processos internos e desenvolvimento de sistemas, a XP trabalha para reduzir os impactos negativos que podem advir da concentração de riscos.

2. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO

A RAS deve ser revisada pelo Comitê de Riscos e aprovada pela Diretoria, anualmente. Se, no decorrer do período, houver mudança de legislação ou procedimento, o documento deverá contemplar a alteração. Após aprovado pela Diretoria, este documento será divulgado internamente.

3. DEFINIÇÕES

Grupo XP Inc.: XP Inc., suas entidades Controladas e Coligadas, consideradas em conjunto.

Acionista Controlador: O acionista ou grupo de acionistas que controlam a Companhia e suas Coligadas, vinculado(s) por acordo ou sob controle comum, que exerça(m) o poder de controle, direto ou indireto, sobre sociedade, nos termos da Lei nº 6.404/76.

Coligadas: As sociedades em que a o Acionista Controlador tenha influência significativa (art. 243, §1º, da Lei nº 6.404/76).

Controladas: As sociedades nas quais a XP Inc. são Acionista Controlador.

Conglomerado Prudencial XP ("XP"): a XP Investimentos CCTVM S.A., Banco XP S.A. e demais empresas do Grupo XP Inc., constituídas no Brasil e no Exterior, que se enquadram na definição que consta da Resolução n° 4.950/2021, do CMN.

Risco: Possibilidade de evento que afeta negativamente a realização dos objetivos ou de seus processos.

Apetite a riscos: Nível de risco que o Conglomerado Prudencial estaria disposto a aceitar na busca e realização de sua estratégia.

RAS: *Risk Appetite Statement* ou declaração de apetite por risco.

Comitê de Riscos: órgão executivo, de caráter permanente, com membros independentes e poderes deliberativos, rege-se por este termo e pela legislação aplicável e tem por objetivo assessorar a administração da instituição, assegurando a aderência dos processos e procedimentos internos com a legislação aplicável e normas regulatórias relacionadas aos assuntos de gerenciamento de riscos, controles internos, segurança da informação, prevenção à fraude, mitigação de riscos, conflito de interesses, assuntos relacionados à risco social, ambiental e climático e a efetividade do gerenciamento contínuo e integrado de riscos de acordo com as Declarações de Apetite por Riscos (RAS), as políticas, os procedimentos e os relatórios gerenciais.

Comitê de Tesouraria: órgão responsável por assegurar que as aplicações do Conglomerado Prudencial XP atendam às regras da estrutura de gerenciamento de risco de mercado, de crédito, de liquidez e de capital.

4. DECLARAÇÃO GERAL DE APETITE A RISCO

A XP estabelece, por meio da RAS, seu apetite a risco para todas as categorias de risco de forma discricionária.

Alinhado com a missão da XP, a estrutura de gestão de risco concentra-se em cinco riscos globais, notadamente:

1. Garantir os mais altos padrões éticos de conduta de todos os colaboradores;
2. Assegurar o cumprimento das obrigações regulamentares vigentes;
3. Salvaguardar a resiliência financeira da XP;
4. Manter um ambiente de controle interno robusto e eficiente; e
5. Preservar a imagem e reputação da XP.

As diretrizes do apetite aos riscos são definidas pela Diretoria da XP, desempenhando suas responsabilidades com o apoio do Comitê de Riscos; de Tesouraria; de Iniciativas Corporativas; de Distribuição de Produtos de Crédito; de Decisão de Crédito; e de Monitoramento de Crédito e Políticas. Por meio dos Comitês, são definidos os objetivos, metas e limites para as unidades de negócio gestoras de riscos, cujas funções incluem a garantia de que suas operações e atividades estejam seguindo as diretrizes dessa RAS. As unidades de controle e gerenciamento de capital, por sua vez, apoiam a administração por meio dos processos de identificação, monitoramento e análise de potenciais inconformidades.

5. PAPÉIS E RESPONSABILIDADES

A eficácia da RAS requer o envolvimento de um vasto grupo de *stakeholders* internos e, em particular, com uma relação de proximidade com a Diretoria Executiva, o Comitê de Riscos e o Diretor de Riscos, sendo definidas funções e responsabilidades para cada um destes *stakeholders* na Política de Gestão Integrada de Riscos da XP, Item *"4. PAPEIS E RESPONSABILIDADES"*, de acordo com os termos da Resolução 4.557.

6. PRINCIPAIS EXPOSIÇÕES E TOLERÂNCIAS AOS RISCOS

Como um elemento fundamental da estrutura de gestão de riscos, a RAS articula o grau de risco que a XP aceitará ao realizar sua missão. As tolerâncias descritas nessa RAS são o resultado de uma análise de impacto e capacidade da companhia gerenciar seus riscos e estão alinhadas com os objetivos e visão da Diretoria.

No âmbito do zelo pela sua reputação e pleno atendimento regulatório, a XP concentra seus esforços na mitigação de potenciais riscos de fraudes internas e externas, vazamento de informações confidenciais, instabilidade e/ou indisponibilidade de sistemas e mantém uma maior prudência em práticas comerciais, a fim de assegurar que o cliente tenha total conhecimento dos produtos de crédito e investimento adquiridos com seus respectivos riscos.

O comportamento da XP em relação aos principais riscos aos quais está exposta é pautado em relação a uma classificação descritiva e quantitativa, quando aplicável, de apetite, a qual demonstra quais são os níveis de risco que está disposta a assumir e a capacidade de gerenciar os riscos de forma eficiente.

A XP definiu seu apetite de risco usando como referência os riscos descritos no artigo 6°, da Resolução 4.557, nominalmente, o risco de crédito, o risco de mercado, o risco operacional, o risco de liquidez e o risco social, ambiental e climático, tais como foram definidos na Resolução 4.557.

A Política de Gestão Integrada de Riscos, Item *"6. GERENCIAMENTO DE RISCOS"*, traz os detalhes e informações relativas aos Riscos observados e gerenciados pela XP.

7. IMPLEMENTAÇÃO DO APETITE AO RISCO

A RAS está integrada na gestão da XP por meio da interdependência com outros exercícios e processos internos, reforçando a utilização das premissas aqui contidas nos principais processos de tomada de decisão.

Cada métrica de apetite ao risco definida possui responsáveis específicos que coordenam as atividades com as unidades de negócio gestoras de riscos, viabilizando a implementação e manutenção de uma estrutura integrada de gerenciamento de riscos no dia a dia das operações e negócios da XP.

Formam indicadores quantitativos que devem ser respeitados pelas áreas de negócios impactadas, conforme definidos abaixo:

7.1 Capital

Limite Interno de Basiléia – Limite mínimo que incorpora *buffer* adicional ao requerimento mínimo de patrimônio de referência regulatório. O detalhamento do *buffer* encontra-se disponível no Plano de Capital.

Os elementos considerados para a definição dos limites de Índice de Basileia são: limites mínimos e colchões adicionais de Patrimônio de Referência, definidos pela Resolução n° 4.958/2021, do CMN, para fazer frente às parcelas regulatórias nos modelos padronizados de risco de crédito, mercado e operacional; apetite de risco ao IRRBB regulatório; apetite de risco por modelo interno ao risco de mercado (VaR); modelos internos de estresse dos riscos de crédito, mercado e operacional.

Razão de Alavancagem – Definida como a razão entre Capital de Nível I e a Exposição Total, calculada nos termos da Circular BACEN 3.748/2015. Na apuração da Exposição Total não é reconhecido nenhum instrumento mitigador de risco de crédito para fins de redução da exposição.

7.2 Risco de Crédito

1. Exposições do Conglomerado Prudencial:

Escopo: concentração em risco de crédito (excluindo soberanos, tesouro nacional, contrapartes centrais) de produtos ativos do Conglomerado Prudencial.

a) Métrica – Limite de Inadimplência:

- Soma do valor financeiro de atrasos de qualquer montante acima de 90 dias em relação ao total das exposições de crédito com clientes pessoa física (PF) e pessoa jurídica (PJ) do Banco XP e da XP Investimentos CCTVM S.A (Corretora).

b) Métrica – Concentração maior emissor de garantias:

- Soma do risco de crédito coberto por emissores dos ativos que constituem as garantias do crédito colateralizado em relação à carteira colateralizada.

c) Métrica – Limite de concentração por contraparte sobre PR:

- Exposição do risco de crédito do maior Grupo Econômico em relação ao Patrimônio de Referência.

d) Métrica – (TOP 10) Limite de concentração por contraparte sobre PR:

- Exposição total do risco de crédito dos 10 maiores Grupos Econômicos em relação ao Patrimônio de Referência.

e) Métrica – (TOP 50) Limite de concentração por contraparte sobre PR:

- Exposição total do risco de crédito dos 50 maiores Grupos Econômicos em relação ao Patrimônio de Referência.

f) Métrica – Limite de exposição por setor estratégico sobre PR:

- Soma das exposições de um setor econômico em relação à carteira clean PJ.
- Os setores econômicos seguem classificação definida em política interna da XP para controle e gestão do risco de crédito.

g) Métrica – Concentração em operações de alto risco

- Soma do valor financeiro das operações com atraso acima de 30 dias; ou

- Soma do valor financeiro de operações *clean* fora do apetite das políticas de concessão de crédito; ou
- A julgamento da área de risco de crédito, baseado na política de concessão dos produtos; em relação carteira total.

7.3 Risco de Mercado

VaR Paramétrico / PR – VaR é o valor em risco de uma carteira e pode ser entendido como uma estimativa de perda máxima em condições normais de mercado. A metodologia adotada é a de *VaR* paramétrico (delta normal), com um intervalo de confiança de 95%, horizonte temporal de 1 dia e sem aplicação de fator de decaimento na volatilidade. O valor final é o VaR em relação ao patrimônio de referência do Conglomerado Prudencial. O limite atual aprovado é de 0.5% do PR.

Teste de Estresse / PR - é o valor obtido a partir do teste de estresse, com base em uma severidade de 99.96% e horizonte temporal de 1 dia, em relação ao patrimônio de referência do Conglomerado Prudencial. O limite atual aprovado é de 4.8% do PR.

Os elementos considerados para a definição dos limites de risco de mercado foram: análise dos retornos históricos dos portfólios pelas respectivas volatilidades realizadas. É com base no histórico dessa métrica (índice Sharpe) que são definidos os níveis de risco a serem adotados.

7.4 Risco de Liquidez

Alocação Floating (Resolução n° 5.008/2022, CMN) – Limite mínimo de ativos elegíveis, segundo a Resolução n° 5.008/2022, CMN, em relação aos recursos de clientes na Corretora.

LCR – Modelo XP – Limite mínimo do indicador LCR (*Liquidity Coverage Ratio*) Modelo XP, que tem como diferencial em relação ao regulatório a exclusão dos recursos de clientes na Corretora da mensuração do indicador.

Os elementos considerados para a definição dos limites de liquidez foram: base normativa ao qual a XP tem obrigatoriedade de cumprimento e; indicador de gestão de liquidez de curto prazo amplamente utilizado no mercado financeiro, porém excluindo um recurso característico do business de Corretora, o qual pode gerar distorções de interpretação dadas suas características particulares.

7.5 IRRBB

Risco de Juros da Carteira Bancária – Considera como limite um % do Patrimônio de Referência. A métrica de acompanhamento é o maior valor entre as estatísticas de Delta EVE e Delta NII, considerando os cenários aprovados em Comitê de Tesouraria (cenários padronizados BACEN ou modelagem interna).

Os elementos considerados para a definição do apetite de riscos de juros da carteira bancária foram: inclusão conjunta das métricas de Delta EVE e Delta NII, como mencionado no artigo 31, da Circular

3.876/2018; e cumprimento das métricas de suficiência de capital, como mencionados no artigo 4, da Circular 3.876/2018.

Adicionalmente, os gestores das áreas de negócio devem seguir as diretrizes e os limites operacionais definidos nas atividades que possam afetar a exposição de risco da empresa. As áreas de controle são as responsáveis por assegurar que a XP atue de acordo com o apetite ao risco definido, evitar a quebra de limites e reportar a posição quantitativa e qualitativa referente às métricas de riscos específicos. Posições que hipoteticamente possam desenquadrar os limites estabelecidos neste documento são levadas aos Comitês específicos do tema e ao Comitê de Riscos para que o planejamento seja mantido.

7.6 Riscos não financeiros

A definição do apetite de riscos não financeiros é estabelecida e revisada anualmente considerando elementos fundamentais inerentes à governança do tema na organização, e consolidada por meio de abordagem de ranqueamento dos principais Riscos.

Na abordagem de ranqueamento dos principais Riscos, anualmente são realizadas reuniões com os principais executivos das áreas de negócio, incluindo o CEO, com o objetivo de capturar as principais preocupações relacionadas aos temas de riscos, à luz dos objetivos estratégicos da empresa.

Além disso a área de riscos não financeiros aplica, sobre as áreas de negócio da empresa, o ciclo de gerenciamento de riscos operacionais composto pelas etapas de Identificação, Mensuração, Classificação, Monitoramento e Reporte de riscos. Os fatores de riscos identificados em cada área de negócio são agrupados em riscos e classificados no mapa da empresa de acordo considerando os resultados das avaliações anteriores, incidentes de riscos ocorridos e requerimentos regulatórios e de mercado.

Para os principais riscos não financeiros da empresa, são definidos indicadores chave de Riscos para monitoramento do comportamento de cada risco relevante. Cada indicador possui tolerâncias compondo o apetite de riscos da organização.

Como resultado da aplicação da abordagem de ranqueamento dos principais Riscos, obtém-se o apetite de riscos não financeiros da organização:

Riscos não financeiros "sem apetite":

- Fraudes internas de qualquer natureza;
- Saída indevida de dinheiro de qualquer natureza;
- Práticas comerciais inadequadas com impacto na venda de produtos em desacordo com a solicitação ou necessidade do cliente;
- Vazamento de dados sensíveis ou estratégicos;
- Descumprimento regulatório de qualquer natureza; e
- Lavagem de dinheiro e financiamento ao terrorismo.

Os demais riscos não financeiros possuem monitoramento acompanhado de suas respectivas tolerâncias, alinhada ao apetite de riscos da organização. O painel RAS que consta do anexo abaixo, seção Risco Operacional, apresenta o detalhamento dos principais indicadores, sendo estes: Perdas Operacionais

(Erro Operacional), Provisão em Processos Cíveis, Tributários, Trabalhistas, Diferença entre Pagamentos versus Provisões em Processos, Perdas por Fraudes Externas das Corretoras, Perdas por Fraudes Externas, Perdas por Fraudes Externas em Cartões, Perdas por Fraudes Externas na Conta Digital.

Perdas operacionais – (Erros Operacionais) – Volume financeiro de perdas operacionais relacionados a falhas internas de processos, sistemas ou pessoas, gerando a necessidade de estornos ou ressarcimentos a clientes.

Provisão em Processos Cíveis, Tributários, Trabalhistas – Volume financeiro relativo à constituição de provisões e atualizações monetárias, sobre os processos cíveis, tributários e trabalhistas.

Diferença entre Pagamentos versus Provisões em Processos – Diferença entre a soma dos pagamentos realizados por acordos e/ou processos judiciais x total das provisões judiciais relativos a esses processos. Representa se as provisões judiciais são suficientes, quando comparadas aos pagamentos.

Perdas por Fraudes Externas das Corretoras – Considera o *Basis Point* (ponto base) relacionado aos casos de fraudes x saída de valores (*cashout*), dos clientes das corretoras (XP, Rico e Clear).

Perdas por Fraudes Externas em Cartões – Considera o *Basis Point* (ponto base), relacionado ao produto cartão de crédito. Soma das perdas confirmadas por fraudes no cartão, dividido pelo faturamento do cartão, multiplicado por 10.000.

Perdas por Fraudes Externas em Conta Digital PIX – Considera o *Basis Point* (ponto base), relacionado ao produto PIX. Soma das perdas confirmadas por fraude, dividido pelo transacional PIX, multiplicado por 10.000.

Perdas por Fraudes Externas na Conta Digital Pagamento – Considera o *Basis Point* (ponto base), relacionado ao produto boleto bancário. Soma das perdas confirmadas por fraudes, divido pelo faturamento por boletos, multiplicado por 10.000.

Adicionalmente, por ter um modelo de negócio fortemente sustentado por canais digitais, a XP direciona especial atenção aos temas de tecnologia e segurança da informação e, consequentemente, definiu um painel de acompanhamento dos principais Indicadores de Riscos de Tecnologia e Segurança da Informação junto às áreas de governança e respectivas diretorias responsáveis, visando monitorar tempestivamente tais indicadores, conforme os limites estratégicos e operacionais estabelecidos, e atuar de forma tempestiva e contínua para evolução destes.

Os gestores das áreas de negócio devem seguir as diretrizes e os limites de tolerância definidos nas atividades que possam afetar a exposição de risco da empresa. As áreas de controle são as responsáveis por assegurar que a XP atue de acordo com o apetite ao risco definido, evitar a quebra de limites e reportar a posição quantitativa e qualitativa referente às métricas de riscos específicos. Posições que hipoteticamente possam desenquadrar os limites estabelecidos neste documento são levadas aos comitês específicos do tema e ao Comitê de Riscos para que o planejamento seja mantido.

8. MONITORAMENTO E REPORTE

O acompanhamento do apetite se dá por meio de processos efetivos de controles, em que os gestores são informados quanto às exposições a riscos e a respectiva utilização dos limites vigentes. O reporte é feito

por meio de sistema de alertas, painel de apetite ao risco, o que facilita a comunicação e destaca as eventuais exceções dos limites.

Em complemento às atividades anteriores, os gestores das áreas de negócio deverão acompanhar os resultados auferidos das métricas apresentadas por tipo de risco, conforme sua responsabilidade.

Este monitoramento é importante para acompanhamento e identificação de possíveis desvios ou quebras de limites definidos neste documento. O monitoramento contínuo deve ser sempre realizado para que as informações sejam reportadas, tempestivamente, e prover aos responsáveis pelas áreas de negócio subsídio suficiente para tomada de decisão, de acordo com as alçadas definidas.

Esta declaração é complementada por uma série de métricas de risco específicas que ajudam a administração a avaliar se os resultados são consistentes com o apetite de riscos da XP. O desempenho em relação a essas métricas é rastreado e relatado regularmente aos comitês aplicáveis e os sistemas de relatórios são mantidos para garantir que o apetite de risco seja efetivamente incorporado nas decisões de gerenciamento.

9. COMUNICAÇÃO

A RAS deve ser disponibilizada e publicada na intranet da XP.

Por força do artigo 56, da Resolução 4.557, o resumo da descrição da estrutura de gerenciamento de riscos e da estrutura de gerenciamento de capital será evidenciado em relatório de acesso público no site da XP em seção específica de informações relativas ao gerenciamento de riscos.

10. EXCEÇÕES

Para os casos de exceção ao cumprimento das regras previstas neste documento, o solicitante deverá apresentar pedido de exceção à Diretoria com as razões que o fundamentam, sendo que a aprovação do pedido deverá ser feita pela Diretoria do Conglomerado XP.

11. ANEXOS

11.1 Painel RAS

a) Conglomerado Prudencial

	Indicadores		Limite
Capital	Índice de Basileia	%	11,50%
	Razão de Alavancagem	%	3,50%
Risco de Crédito	Limite de Inadimplência	%	5%
	Concentração maior emissor de garantias (crédito colateralizado)	%	10%
	Limite de concentração por contraparte sobre PR	%	25%
	(TOP 10) Limite de concentração por contraparte sobre PR	%	120%
	Limite de exposição por setor estratégico sobre Carteira	%	50%
	Concentração em operações de alto risco	%	10%
Risco de Liquidez	Alocação Floating (Res. 5.008)	%	100%
	LCR Prudencial - Modelo XP	%	100%
Risco de Mercado	TRADING - VaR Diário (% sobre o Patrimônio de Referência)	%	0,5%
	TRADING - Teste de Estresse Diário (% sobre o Patrimônio de Referência)	%	4,8%
Risco Operacional	Perdas Operacionais (Erro Operacional)	MM	25
	Provisão em Processos Cíveis, Tributários e Trabalhistas	MM	25
	Diferença entre Pagamentos vs Provisões em Processos	MM	10
	Perdas por Fraudes Externas - Corretora - XP	BP	0,45
	Perdas por Fraudes Externas - Corretora - RICO	BP	0,45
	Perdas por Fraudes Externas - Corretora - Clear	BP	0,45
	Perdas por Fraudes Externas - Cartões	BP	5,5
	Perdas por Fraudes Externas - Conta Digital - PIX	BP	2,4
	Perdas por Fraudes Externas - Conta Digital - Pgto	BP	2,1
IRRBB	Limite para Risco de Juros da Carteira Bancária (IRRBB)	%	15%
Risco Social, Ambiental e Climático	Exposição a Risco Social, Ambiental e Climático do Portfolio de Crédito PJ	%	10%
	Sensibilidade Climática do Portfólio de Crédito PJ	%	15%

b) Grupo XP Inc.

	Indicadores		Limite
Capital	Índice de Basileia	%	13,50%
Risco de Crédito	Limite de Inadimplência	%	5%
	Concentração maior emissor de garantias (crédito colateralizado)	%	10%
	Limite de concentração por contraparte sobre PR	%	10%
	(TOP 10) Limite de concentração por contraparte sobre PR	%	60%
	(TOP 50) Limite de concentração por contraparte sobre PR	%	120%
	Limite de exposição por setor estratégico sobre Carteira	%	50%
	Concentração em operações de alto risco	%	10%
Risco de Liquidez	Alocação Floating (Res. 5.008)	%	100%
	LCR - Modelo XP	%	100%
Risco de Mercado	TRADING - VaR Diário (% sobre o Patrimônio de Referência)	%	0,5%
	TRADING - Teste de Estresse Diário (% sobre o Patrimônio de Referência)	%	4,8%
Risco Operacional	Perdas Operacionais (Erro Operacional)	MM	25
	Provisão em Processos Cíveis, Tributários e Trabalhistas	MM	25
	Diferença entre Pagamentos vs Provisões em Processos	MM	10
	Perdas por Fraudes Externas - Corretora - XP	BP	0,45
	Perdas por Fraudes Externas - Corretora - RICO	BP	0,45
	Perdas por Fraudes Externas - Corretora - Clear	BP	0,45
	Perdas por Fraudes Externas - Cartões	BP	5,5
	Perdas por Fraudes Externas - Conta Digital - PIX	BP	2,4
	Perdas por Fraudes Externas - Conta Digital - Pgto	BP	2,1
IRRBB	Limite para Risco de Juros da Carteira Bancária (IRRBB)	%	5%
Risco Social, Ambiental e Climático	Exposição a Risco Social, Ambiental e Climático do Portfolio de Crédito PJ	%	10%
	Sensibilidade Climática do Portfólio de Crédito PJ	%	15%

11.2 Painel de indicadores de riscos de tecnologia e segurança da informação

APETITE DE RISCO TECH, CYBER & CONTINUIDADE

KRIs – Indicadores de Riscos

Vulnerabilidades

Indicador (KRI)	Limite 🔴	Tolerância 🟡	Gatilho 🟡	Alvo 🟢
3.1 Vulnerabilidades de Infra (Crítica) em Aberto + 90 Dias – Área Owner TI	4%	2%	1%	0%
3.2 Vulnerabilidades de Infra (Crítica) em Aberto + 90 Dias - Área Owner Rico	4%	2%	1%	0%
3.3 Vulnerabilidades de Infra (Crítica) em Aberto + 90 Dias - Área Owner XP US	4%	2%	1%	0%
3.4 Vulnerabilidades de Infra (Crítica) em Aberto + 90 Dias - Grupo Respónsável Log4j*	4%	2%	1%	0%
3.5 Vulnerabilidades de Infra (Crítica) em Aberto + 90 Dias - EOL	5%	4%	3%	2%
3.6 Vulnerabilidades BD (Crítica) - Exadata em Aberto + 360 Dias – Grupo Responsável Banco de Dados	4%	2%	1%	0%
3.7 Vulnerabilidades Redes (Crítica) em Aberto + 180 Dias – Área Owner TI	4%	2%	1%	0%
3.8 Vulnerabilidades Ambiente Tesouraria (Crítica) em Aberto + 90 Dias	5%	4%	3%	2%
3.9 Vulnerabilidades de Aplicações (Críticas) em Aberto + 90 Dias	4%	2%	1%	0%
3.10 Vulnerabilidades de Infra (Alta) em Aberto + 90 Dias – Área Owner TI	5%	4%	3%	2%
3.11 Vulnerabilidades de Infra (Alta) em Aberto + 90 Dias - Área Owner Rico	5%	4%	3%	2%
3.12 Vulnerabilidades de Infra (Alta) em Aberto + 90 Dias - Área Owner XP US	5%	4%	3%	2%

Indicador (KRI)	Limite 🔴	Tolerância 🟡	Gatilho 🟡	Alvo 🟢
3.13 Vulnerabilidades de Infra (Alta) em Aberto + 90 Dias - Grupo Responsável Log4j	5%	4%	3%	2%
3.14 Vulnerabilidades de Infra (Alta) em Aberto + 90 Dias – EOL	5%	4%	3%	2%
3.15 Vulnerabilidades BD (Alta) - Exadata em Aberto + 360 Dias – Grupo Responsável Banco de Dados	5%	4%	3%	2%
3.16 Vulnerabilidades Redes (Alta) em Aberto + 180 Dias – Área Owner TI	5%	4%	3%	2%Jun
3.17 Vulnerabilidades Ambiente Tesouraria (Alta) em Aberto + 90 Dias	5%	4%	3%	2%
3.18 Vulnerabilidades de Aplicações (Altas) em Aberto + 90 Dias	4%	2%	1%	0%
3.19 Hardening – Equipamentos de Rede	93%	95%	97%	99%
3.20 Hardening – End-User	93%	95%	97%	99%
3.21 Hardening – Banco de Dados	85%	88%	90%	92%
3.22 Hardening – Servidores	93%	95%	97%	99%

**Após análise do time de redteam, as vulnerabilidades de Log4j foram classificadas, em março/23, com a severidade Média. Portanto não serão mais acompanhadas no apetite de risco.*

[CLASSIFICAÇÃO: INTERNA]

APETITE DE RISCO TECH, CYBER & CONTINUIDADE

KRIs – Indicadores de Riscos

Obsolescência

Indicador (KRI)	Limite 🔴	Tolerância 🟡	Gatilho 🟡	Alvo 🟢
1.1 Obsolescência OS (Servidores – Microsoft e Linux)	10%	8%	6%	5%
1.2 Obsolescência OS End-User (Windows e MAC)	10%	8%	6%	5%
1.3 Obsolescência BD Oracle Exadata (Ambientes Produtivos)	10%	8%	6%	5%
1.4 Obsolescência BD SQL / NoSQL (MongoDB)	10%	8%	6%	5%
1.5 Obsolescência HW (Data Center: Bare Metal; Hiperconvergência; Hardware de Backup e Storage (Discos, SAN e Tape Library)	10%	8%	6%	5%
1.6 Obsolescência Aplicações	18%	15%	12%	10%
1.7 Obsolescência HW End-User (Máquinas Dell e MAC)	10%	8%	6%	4%
1.8 Obsolescência SW End-User (Softwares uso básico, navegadores)	10%	8%	6%	4%
1.9 Obsolescência Ferramentas de Monitoração de Segurança	6%	4%	2%	0%
1.10 Obsolescência HW (Equipamentos de Rede: switches, roteadores, balanceadores)	8%	6%	4%	2%

KRIs – Indicadores de Riscos

Disponibilidade

Indicador (KRI)	Limite 🔴	Tolerância 🟡	Gatilho 🟡	Alvo 🟢
2.1 Serviços de Negócio Críticos com Contingência de Desastre (%)	90%	93%	96%	100%
2.2 Disponibilidade de Serviços Negócio Missão Crítica (%)	99,70%	99,80%	99,85%	99,90%
2.3 Disponibilidade de Serviços Negócio Críticos (%)	99,50%	99,60%	99,70%	99,80%
2.4 Incidentes Graves (P1 e P2)	4	2	1	0
2.5 Change Failure Rate Serviços Negócio Críticos e Missão Crítica	4%	3%	2%	1%
2.6 MTTR Serviços Negócio Críticos e Missão Crítica	3,5 h	3 h	2,5 h	2 h

[CLASSIFICAÇÃO: INTERNA]

ANEXO I

Documentos mencionados

- Política de Gestão Integrada de Riscos
- Plano de Capital

Referências Regulatórias

- Resolução nº 4.557/17, do Conselho Monetário Nacional
- Resolução n° 4.958/2021, do Conselho Monetário Nacional
- Resolução n° 5.008/2022, do Conselho Monetário Nacional
- Circular BACEN 3.748/ 2015
- Circular BACEN 3.876/2018