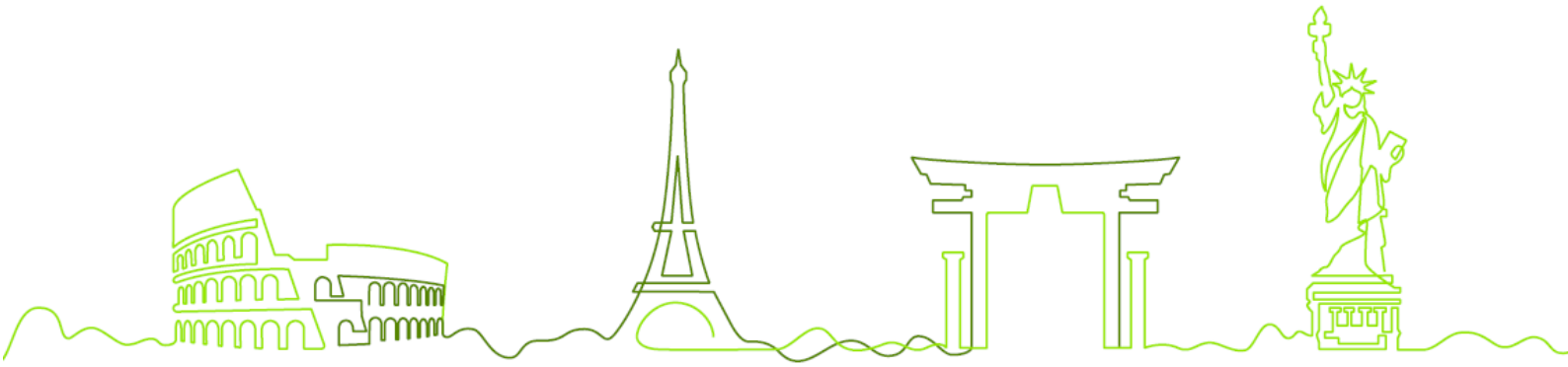

Política de Segurança de Recursos Humanos

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	30 abr 2025	Cibersegurança	Versão Original

Sumário

1. Objetivo

Esta Política tem o objetivo de garantir que funcionários e prestadores de serviços do Intex Bank Banco de Câmbio S/A, referenciado abaixo somente como “Intex Bank”, atendam aos requisitos de segurança, compreendam suas responsabilidades e estejam qualificados para suas funções, além de estabelecer diretrizes que minimizem riscos e respeitem os requisitos de segurança durante o processo de admissão, gestão e demissão de colaboradores do “Intex Bank”.

2. Escopo

Esta Política se aplica a todos os funcionários do “Intex Bank”, consultores, prestadores de serviços e outras entidades terceirizadas com acesso às redes de produção e aos recursos de sistema do “Intex Bank”.

3. Requisitos

As verificações de antecedentes dos funcionários do “Intex Bank” devem ser realizadas de acordo com as leis e regulamentos pertinentes, devendo ser proporcionais aos requisitos de negócios, à classificação das informações a serem acessadas e aos riscos percebidos. A análise dos antecedentes pode incluir verificações criminais, desde que não sejam proibidas pela legislação local.

Todos os terceiros com acesso técnico privilegiado ou administrativo a sistemas ou redes de produção do “Intex Bank” estão sujeitos a uma verificação de antecedentes ou à exigência de fornecer evidências de um histórico aceitável, com base no nível de acesso e no risco percebido para a organização.

Esta Política está alinhada às exigências do Banco Central do Brasil, especialmente as Resoluções BCB nº 85/2021 e nº 139/2021, a Resolução CMN nº 4.893/2021, e a Resolução CMN nº 5.088/2023, que tratam da segurança da informação, gestão de incidentes e continuidade de negócios. Também observa a Circular nº 3.909/2018, relacionada ao tratamento de dados e prevenção de vazamentos.

Adicionalmente, adota boas práticas internacionais, como o NIST Cybersecurity Framework (CSF), as normas ISO/IEC 27001:2022, 27002 e 27701, e o padrão PCI DSS para proteção de dados de pagamento. Está em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com a Lei nº 9.613/1998, no contexto de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo, incluindo controles tecnológicos e monitoramento de fraudes.

4. Competência e Avaliação de Desempenho

A equipe de recursos humanos e o gerente de contratação ou seus representantes devem avaliar as habilidades e competências dos funcionários e prestadores de serviços durante o processo de contratação. As habilidades e competências necessárias devem constar nas descrições e requisições de cargos, alinhadas com as responsabilidades descritas na matriz de responsabilidades. As avaliações de competência podem incluir verificações de referências, verificações de formação acadêmica e certificação, testes técnicos e entrevistas.

Todos os funcionários do "Intex Bank" passarão por uma avaliação de desempenho semestral na qual se avalia o desempenho no trabalho, a competência na função, a adesão às políticas e ao código de conduta da empresa e o cumprimento dos objetivos específicos da função.

5. Termos e Condições de Emprego

As políticas da empresa e as funções e responsabilidades de segurança da informação devem ser comunicadas aos funcionários e terceiros no momento da contratação. Os funcionários e prestadores de serviço devem confirmar formalmente sua compreensão e aceitação das responsabilidades pela segurança, além de assinarem o termo de responsabilidade e confidencialidade presente no anexo 1. Os funcionários e terceiros com acesso a informações da empresa ou dos clientes devem assinar acordos apropriados de não divulgação, confidencialidade e código de conduta. Os acordos contratuais devem declarar as responsabilidades pela segurança das informações, conforme necessário. Os funcionários e terceiros pertinentes devem seguir todas as políticas de segurança da informação do "Intex Bank".

Ao ser realizado a contratação de um novo funcionário ou prestador de serviço que deva ter acesso aos sistemas do "Intex Bank", o RH ou gestor da área deve preencher o formulário para concessão de acessos ao colaborador, onde a TI irá deliberar os mesmos.

6. Responsabilidades da Gerência

A gerência será responsável por garantir que as políticas e os procedimentos de segurança da informação sejam revisados anualmente, distribuídos e disponibilizados, e que os funcionários e prestadores de serviços cumpram estas políticas e procedimentos durante o período do emprego ou contrato. A revisão da política anual deve incluir uma análise de todos os procedimentos, padrões ou diretrizes vinculados ou referenciados.

A gerência deve assegurar que as responsabilidades pela segurança da informação sejam comunicadas aos indivíduos por meio de descrições de funções e políticas por escrito ou qualquer outro método documentado que seja atualizado e mantido de forma precisa. A conformidade com as políticas e os procedimentos de segurança da informação e o cumprimento das responsabilidades de segurança da informação devem ser avaliados durante o processo de análise de desempenho, sempre que aplicável.

Informações pessoais de clientes, funcionários e terceiros que tenham contrato com o "Intex Bank", devem ser armazenadas em local adequado e protegido com os controles próprios à sua classificação, conforme a Política de Classificação das Informações.

A gerência deve considerar as pressões excessivas e as oportunidades de fraude ao estabelecer incentivos e separar funções, responsabilidades e autoridades.

7. Conscientização, Educação e Treinamento sobre Segurança da Informação

Todos os funcionários do "Intex Bank" e terceiros com acesso técnico administrativo ou confidencial aos sistemas e redes de produção do "Intex Bank" devem realizar o treinamento de conscientização sobre segurança no momento da contratação e, depois, com periodicidade anual. A gerência supervisionará a realização do treinamento e tomará as medidas adequadas para assegurar o cumprimento desta Política. Os funcionários e prestadores de serviço devem estar cientes das políticas e procedimentos relevantes sobre segurança da informação e privacidade de dados. A empresa deve garantir que a equipe receba o treinamento adequado sobre segurança e privacidade de dados, de acordo com suas funções e responsabilidades.

Para manter um nível robusto de conscientização sobre segurança, a empresa fornecerá atualizações e comunicados relacionados à segurança dos funcionários de forma contínua por meio de vários canais de comunicação, conforme necessário.

Os líderes e gerentes de segurança da informação devem garantir um desenvolvimento profissional adequado para que haja uma compreensão das ameaças e tendências atuais no cenário da segurança. Os líderes de segurança e as principais partes interessadas devem participar de treinamentos, obter e manter certificações relevantes e manter a associação em grupos do setor, conforme apropriado.

8. Processo de Rescisão

Os processos de rescisão e desligamento de funcionários e prestadores de serviço devem

garantir que o acesso físico e lógico seja imediatamente revogado, de acordo com os SLAs e as políticas da empresa, e que todos os equipamentos fornecidos pela empresa sejam devidamente devolvidos, para que os acessos dos colaboradores que estão em sendo desligados sejam devidamente revogados, o RH ou gestor da área deve preencher o formulário de bloqueio de acesso. Este processo deve ser documentado por meio do checklist de *offboarding*, anexo na ferramenta *ClickCompliance*.

Quaisquer acordos de segurança ou confidencialidade que permaneçam válidos após a rescisão devem ser comunicados ao funcionário ou prestador de serviço no momento da rescisão.

9. Processo Disciplinar

Os funcionários e terceiros que violarem as políticas de segurança da informação do "Intex Bank" estarão sujeitos ao processo disciplinar progressivo do "Intex Bank", que poderá incluir a rescisão do contrato de trabalho.

10. Exceções

Exceções a esta Política devem ser formalmente submetidas ao Gestor de TI e/ou ao Diretor Administrativo para avaliação e aprovação, garantindo que cada caso seja devidamente documentado e justificado.

Em casos de dúvidas, comentários ou necessidade de exceções, entre em contato pelo e-mail suporte@intexbank.com.br.

11. Violações e Não Cumprimento da Política

Qualquer violação das diretrizes estabelecidas nesta Política deverá ser comunicada imediatamente ao Gestor de TI, Diretor Administrativo e ao Encarregado de Proteção de Dados para as providências cabíveis. Violações poderão resultar em sanções administrativas, incluindo a perda de privilégios de acesso a sistemas e redes, bem como medidas disciplinares conforme os procedimentos internos do "Intex Bank", que podem incluir rescisão de contratos ou parcerias.

12. Vigência

Esta política entra em vigor na data de sua publicação, sendo revisada no prazo de 18 (dezoito) meses, ou a qualquer momento, conforme a necessidade.

São Paulo, 05 de junho de 2025.

O presente documento foi aprovado pelo Comitê Diretivo conforme Ata de Reunião realizada em 05/06/2025.

ANEXOS

ANEXO 1 – TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Eu, **[INSERIR NOME COMPLETO DO COLABORADOR]**, CPF **[INSERIR CPF]**, cargo **[INSERIR CARGO]**, declaro, perante o **INTEX BANK BANCO DE CÂMBIO S/A**, estar ciente e concordar integralmente com este Termo de Responsabilidade e Confidencialidade, referente ao uso de recursos da empresa e acesso a sistemas críticos:

1. USO DE RECURSOS: O uso dos recursos da empresa (equipamentos, softwares, sistemas, redes, e-mail, informações) destina-se exclusivamente a fins laborais. O uso para outros propósitos é proibido.

2. ENCERRAMENTO E CONFIDENCIALIDADE: Ao término do contrato, informarei e entregarei todos os ativos produzidos ou sob minha responsabilidade, garantindo sua integridade e disponibilidade aos funcionários com direito de acesso. Manterei confidencialidade das informações e ativos da empresa por no mínimo 5 anos após o encerramento do contrato.

3. MONITORAMENTO: Concordo que a empresa pode analisar, auditar, interceptar, acessar e divulgar dados trafegados ou armazenados em seus sistemas a qualquer momento, com ou sem aviso, dentro ou fora do expediente.

4. CONSEQUÊNCIAS: A violação deste termo sujeita-me a medidas disciplinares administrativas e/ou legais, incluindo desligamento.

5. ACESSO A SISTEMAS CRÍTICOS: Ciente das normas internas sobre ACESSO A SISTEMAS CRÍTICOS (sistemas internos, diretórios restritos, informações públicas e confidenciais essenciais). O acesso somente será realizado por recursos próprios da empresa, sendo vedado o uso de dispositivos ou redes externas não autorizadas (exceto com autorização formal).

SISTEMAS CRÍTICOS:

- Listar sistemas críticos utilizados pelo colaborador

DECLARAÇÃO DE CONFIDENCIALIDADE E RESPONSABILIDADE

Comprometo-me a:

a) Tratar adequadamente as informações acessadas, utilizando-as para fins profissionais, conforme normas internas e legislação (LGPD).
b) Não praticar atos que comprometam a confidencialidade, integridade ou disponibilidade das informações nos sistemas críticos.
c) Não copiar, reproduzir ou divulgar informações confidenciais sem autorização formal ou obrigação legal.
d) Utilizar os sistemas críticos exclusivamente para minhas funções profissionais.
e) Proteger minhas credenciais de acesso (VPN e MFA), não compartilhando senhas.
f) Comunicar imediatamente incidentes de segurança, acessos indevidos ou violações.

CONDIÇÕES DE USO E LIMITAÇÕES:

1. Acesso aos sistemas críticos e diretórios internos somente por recursos próprios da empresa.
2. Proibido o uso de dispositivos e contas pessoais/redes não corporativas para acessar informações críticas (salvo autorização formal).
3. O acesso aos sistemas críticos é monitorado continuamente e pode ser auditado sem aviso prévio.
4. Uso indevido dos sistemas (instalação de softwares não autorizados, alteração de segurança) resultará em sanções.

RESPONSABILIDADE E DESCUMPRIMENTO:

Sou integralmente responsável pelo uso seguro e adequado dos sistemas críticos. A violação deste termo resultará em sanções disciplinares, civis e penais, conforme legislação e normas internas. Informarei imediatamente sobre encerramento de vínculo ou mudança de função para revogação de acessos.

VIGÊNCIA: Este termo é válido enquanto eu tiver acesso aos sistemas críticos do **INTEX BANK**. A cessação do acesso não elimina a responsabilidade pela confidencialidade das informações acessadas.

DECLARAÇÃO DE ACEITAÇÃO:

Li, compreendi e aceito os termos deste Termo de Responsabilidade do **INTEX BANK BANCO DE CÂMBIO S/A**.

Local e data.

_____

[INSERIR NOME COMPLETO DO COLABORADOR]
[INSERIR CARGO]
[INSERIR CPF]