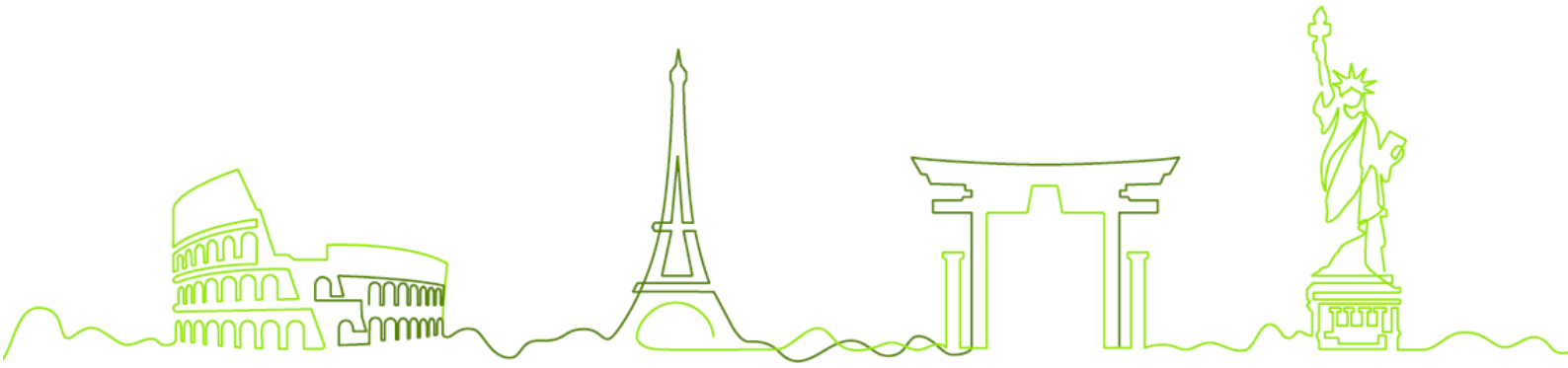

Política de Segurança da Informação

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	Abril / 2018	Tecnologia da Informação	Versão Original
2.0	Abril / 2021	Tecnologia da Informação	Atualização
3.0	Julho / 2022	Tecnologia da Informação	Atualização
4.0	Julho / 2023	Tecnologia da Informação	Atualização
5.0	Abril / 2025	Cibersegurança / Tec. da Informação	Atualização

Sumário

1. Objetivo

Esta política visa proteger o Intex Bank Banco de Câmbio S/A, referenciada abaixo como "Intex Bank", seus funcionários e parceiros de ações ilegais ou prejudiciais por indivíduos, de forma ou não deliberada.

Os sistemas relacionados à Internet/Intranet/Extranet, incluindo, entre outros, equipamentos de informática, software, sistemas operacionais, mídia de armazenamento, contas de rede que oferecem correio eletrônico, navegação na web e transferência de arquivos, são de propriedade do "Intex Bank". Esses sistemas devem ser usados para os fins de negócios que atendam aos interesses da empresa e de nossos clientes e consumidores no curso das operações normais.

A segurança eficaz envolve a participação e o apoio de todos os funcionários e terceirizados do "Intex Bank" que lidam com informações e/ou sistemas de informação. É responsabilidade de cada membro da equipe ler e entender esta política e conduzir suas atividades de acordo com ela.

2. Escopo

Esta Política cobre o uso de informações, aparelhos eletrônicos e de computação e recursos de rede para o "Intex Bank" conduzir negócios ou interagir com redes internas e sistemas de negócios, sejam de propriedade ou alugados pelo "Intex Bank", o funcionário ou um terceiro. Todos os funcionários, terceirizados, consultores, estagiários e outros funcionários do "Intex Bank" e suas subsidiárias devem ter bom senso em relação ao uso apropriado das informações, aparelhos eletrônicos e recursos de rede de acordo com as políticas e normas do "Intex Bank" e das leis e regulamentos locais.

Esta política abrange funcionários, prestadores de serviços, consultores, temporários e outros trabalhadores do "Intex Bank", incluindo todo o pessoal afiliado a terceiros. Esta política cobre todos os dados controlados pelo "Intex Bank", incluindo dados dos clientes; bem como a todos os equipamentos, sistemas, redes e softwares de propriedade ou alugados pelo "Intex Bank".

Esta Política está alinhada com a Resolução CMN nº 4.893/2021 e a Resolução BCB nº 85/2021, que determinam a adoção de uma estrutura robusta de segurança cibernética e práticas de governança para proteção de dados e gestão de riscos operacionais. Adota, ainda, as melhores práticas preconizadas pelo NIST Cybersecurity Framework (CSF) e pela ISO/IEC 27001:2022, referências globais para a implementação de sistemas de gestão da segurança da informação (SGSI) e controles protetivos. Também reforça a conformidade

com a LGPD (Lei nº 13.709/2018), assegurando o tratamento seguro de dados pessoais, e com a Lei nº 9.613/1998, ao estabelecer controles que contribuem para a prevenção à lavagem de dinheiro. Dessa forma, esta política sustenta a integridade, disponibilidade e confidencialidade das informações, promovendo a continuidade dos negócios e a mitigação de riscos cibernéticos.

3. Relatórios de Incidentes de Segurança

Todos os usuários devem relatar eventos ou incidentes de segurança conhecidos ou suspeitos, inclusive violações nas políticas e vulnerabilidades observadas na segurança. Os incidentes devem ser comunicados imediatamente ou o quanto antes via e-mail para: suporte@trevisocc.com.br.

No e-mail, descreva o incidente ou observação juntamente com quaisquer detalhes relevantes.

4. Denúncia de Fraude Anônima

Nossa política de denúncias visa a incentivar e permitir que funcionários e outras pessoas abram chamados para questões sérias de forma interna para abordarmos e corrigirmos condutas e ações inadequadas. É responsabilidade de todos os funcionários denunciar violações ao nosso código de ética ou suspeitas de violação de leis ou regulamentos que regem nossas operações.

É contrário aos nossos valores que alguém faça retaliação a qualquer funcionário ou a quem, de boa-fé, denuncie uma violação à ética ou à suspeita de violação da lei, seja em forma de reclamação de discriminação, suspeita de fraude ou suspeita de violação de qualquer regulamento. O funcionário que retaliar alguém que, de boa-fé, tenha denunciado uma violação está sujeito a medidas disciplinares que incluem a rescisão do contrato de trabalho.

Denúncias anônimas podem ser enviadas pelo link: https://trevisocambio.com.br/canal-de-denuncia/.

5. Política de Dispositivos Móveis

Todos os aparelhos dos usuários finais (telefones celulares, tablets, laptops, desktops etc.) devem seguir esta política. Os funcionários devem ter extremo cuidado ao abrir o anexo de um e-mail recebido de remetentes desconhecidos, pois pode conter malware.

As senhas no nível do sistema e no nível do usuário devem seguir a Política de Controle de Acesso. É proibido dar acesso a outro indivíduo, deliberadamente ou devido a falha na proteção de um aparelho.

Todos os aparelhos dos usuários finais, sejam pessoais (BYOD) ou de propriedade da empresa, usados para acessar os sistemas de informação do "Intex Bank" (e-mail etc.) devem aderir às regras e aos requisitos a seguir:

a) Os aparelhos devem ter um protetor de tela protegido por senha (ou controle equivalente, como biométrico) ou bloqueio de tela após 5 minutos inativo**.**

b) Os aparelhos devem ser bloqueados sempre que deixados sem supervisão**.**

c) Os usuários devem relatar imediatamente qualquer suspeita de uso indevido ou roubo de um aparelho móvel para o departamento de TI do "Intex Bank".

d) As informações confidenciais não podem ser guardadas nos aparelhos móveis nem nas unidades USB (exceto dados para contato de negócios, como nomes, números de telefone e endereços de e-mail)**.**

e) Nenhum aparelho móvel usado para acessar os recursos da empresa (como compartilhamentos de arquivos e e-mail) deve ser compartilhado com nenhuma outra pessoa**.**

f) Após a rescisão, os usuários concordam em devolver todos os aparelhos de propriedade da empresa e apagar todas as informações e contas da empresa de quaisquer aparelhos pessoais**.**

6. Política de Tela e Mesa Limpas

Os usuários não devem deixar material confidencial sem segurança na mesa nem no espaço de trabalho; e devem garantir que as telas estejam bloqueadas quando não estiverem em uso.

7. Política de Acesso e Trabalho Remoto

Trabalho remoto se refere a qualquer situação em que o pessoal organizacional opera fora do escritório. Isso inclui teletrabalho, local de trabalho flexível, ambientes de trabalho virtuais e manutenção remota. Laptops e outros recursos de computador usados para acessar a rede do "Intex Bank" devem cumprir os requisitos de segurança descritos nas políticas de segurança da informação do "Intex Bank" e aderir às seguintes normas:

a) As regras da empresa devem ser seguidas durante o trabalho remoto, incluindo protocolos de mesa limpa, impressão, descarte de ativos e relatórios de eventos de segurança da informação, a fim de evitar o manuseio incorreto ou a exposição acidental de informações confidenciais.

b) Para que os aparelhos móveis não conectem nenhum aparelho violado à rede da empresa, as políticas de antivírus exigem o uso e a aplicação de software antivírus pelo cliente.

c) O software antivírus deve detectar e impedir ou colocar em quarentena softwares mal-intencionados, realizar escaneamentos periódicos no sistema e estar com as atualizações automáticas ativadas.

d) Para evitar possíveis ataques de espionagem ou de intermediários, exija o uso de VPN ao transmitir informações confidenciais por qualquer rede Wi-Fi que não sejam do "Intex Bank".

e) Ao trabalhar em uma rede doméstica, veja se as configurações padrão de Wi-Fi foram alteradas, como nome, senha e acesso do administrador**.**

f) Para o administrador do sistema, é recomendável configurar uma rede específica para o trabalho com criptografia WPA3 forte ou, no mínimo, WPA2 com senha robusta, juntamente com a configuração de uma VLAN dedicada, se possível. Além disso, o WPS (Wi-Fi Protected Setup) e o UPnP (Universal Plug and Play) devem ser desativados se não forem especificamente necessários**.**

g) Os usuários só devem se conectar a uma rede externa se houver firewall de software seguro e atualizado configurado no computador móvel**.**

h) Os usuários estão proibidos de alterar ou desativar qualquer controle de segurança organizacional, como firewalls pessoais, software antivírus em sistemas usados para acessar os recursos do "Intex Bank".

i) É permitido o uso de softwares e/ou serviços de acesso remoto (cliente VPN etc.) desde que seja fornecido pela empresa e configurado com uma autenticação multifatorial (MFA)**.**

j) Não podem ser usadas nem instaladas tecnologias de acesso remoto não autorizadas em nenhum sistema do "Intex Bank".

k) Os usuários não devem transmitir informações confidenciais em um Wi-Fi público.

8. Política de Uso Inaceitável

Informações próprias do "Intex Bank" e dos clientes guardadas em aparelhos eletrônicos e

de computação, sejam de propriedade ou alugadas pelo “Intex Bank”, o funcionário ou um terceiro, permanecem como propriedade exclusiva do “Intex Bank” para os fins desta política. Os funcionários e terceirizados devem assegurar, por meios legais ou técnicos, que as informações próprias sejam protegidas de acordo com a Política de Classificação de Informações. Aos usuários de laptops ou aparelhos disponibilizados pela empresa, é exigido o uso do sistema de compartilhamento de arquivos da empresa para guardar os arquivos de negócios. Guardar documentos importantes no compartilhamento de arquivos é um meio de "fazer backup" do seu laptop.

O usuário é responsável por denunciar imediatamente o roubo, perda ou divulgação não autorizada de informações ou equipamentos do “Intex Bank”. O acesso, uso ou compartilhamento de informações de propriedade do “Intex Bank” somente é permitido de forma autorizada e na medida necessária para o desempenho das funções de trabalho. Os funcionários devem ter bom senso em relação ao uso pessoal dos aparelhos fornecidos pela empresa.

Para segurança e manutenção da rede, indivíduos autorizados do “Intex Bank” podem monitorar equipamentos, sistemas e tráfego de rede a qualquer momento.

O “Intex Bank” reserva o direito de auditar periodicamente redes e sistemas para garantir o cumprimento desta política.

8.1. Uso Inaceitável

Em geral, as atividades a seguir são proibidas. Os funcionários podem ser isentos dessas restrições durante o curso das responsabilidades legítimas de trabalho, com a aprovação da gerência devidamente documentada. Em nenhum caso um funcionário do “Intex Bank” está autorizado a se envolver em qualquer atividade ilegal de acordo com as leis locais, estaduais, federais ou internacionais enquanto utilizar os recursos de propriedade do “Intex Bank” ou enquanto representar o “Intex Bank” em qualquer capacidade. A lista abaixo não é completa, mas traz uma estrutura das atividades que se enquadram na categoria de uso inaceitável.

As seguintes atividades, sem exceção, são estritamente proibidas:

a) Violação dos direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredos comerciais, patentes ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, entre outros, a instalação ou distribuição de "produtos de software pirateados" ou outros produtos de software que não estejam devidamente licenciados para uso pelo “Intex Bank”.

b) Cópia não autorizada de material protegido por direitos autorais, incluindo, entre outros, digitalização e distribuição de fotografias de revistas, livros e outras fontes protegidas por direitos autorais, música protegida por direitos autorais e instalação de qualquer software protegido por direitos autorais para o qual o "Intex Bank" ou o usuário final não tenha uma licença ativa**.**

c) É proibido acessar dados, servidores e contas para qualquer finalidade que não seja a de conduzir os negócios do "Intex Bank", mesmo com acesso autorizado.

d) É ilegal a exportação de software, informações técnicas, software de criptografia ou tecnologia, em violação às leis internacionais ou regionais de controle de exportação. A gerência apropriada será consultada antes da exportação de qualquer material em questão**.**

e) Introdução de programas maliciosos na rede ou nos sistemas (vírus, worms, cavalos de Troia, bombas de e-mail etc.)**.**

f) Revelar a senha da sua conta a outras pessoas ou permitir o uso da sua conta por outras pessoas. Isso inclui os parentes se o trabalho for feito em casa**.**

g) Usar um ativo de computação do "Intex Bank" para se envolver ativamente na aquisição ou transmissão de material que viole as leis de assédio sexual ou de local de trabalho hostil**.**

h) Fazer ofertas fraudulentas de produtos, itens ou serviços provenientes de uma conta do "Intex Bank".

i) Fazer afirmações sobre a garantia, de forma expressa ou não, a menos que seja parte das tarefas normais do trabalho**.**

j) Efetuar violações na segurança ou interferência na comunicação da rede. As violações na segurança incluem, entre outros, acessar dados dos quais o funcionário não é o destinatário pretendido ou fazer login em um servidor ou conta que o funcionário não tem autorização expressa para acessar, a menos que essas tarefas entrem no escopo das tarefas regulares. Para os fins desta seção, "interferência" inclui, entre outros, sniffing de rede, pinged floods, packet spoofing, negação de serviço e informações de roteamento forjadas para fins maliciosos**.**

k) É expressamente proibido o escaneamento de portas ou de segurança, a menos que haja um aviso prévio à equipe de engenharia do "Intex Bank".

l) Executar qualquer forma de monitoramento na rede que intercepte dados não destinados ao host do funcionário, a menos que essa atividade faça parte do trabalho normal do funcionário**.**

m) Contornar a autenticação do usuário ou a segurança de qualquer host, rede ou conta.

n) Introduzir honeypots, honeynets ou tecnologia semelhante na rede de “Intex Bank”.

o) Interferir ou negar serviço a qualquer usuário que não seja o host do funcionário (ataque de negação de serviço etc.).

p) Usar qualquer programa/script/comando, ou enviar mensagens de qualquer tipo, com a intenção de interferir ou desativar a sessão de um usuário, por qualquer meio.

q) Dar informações ou listas relativas funcionários, terceirizados, parceiros ou clientes do “Intex Bank” a partes externas sem a autorização do “Intex Bank”.

9. E-mail e atividades de Comunicação

O uso do correio eletrônico do “Intex Bank” é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o “Intex Bank” e não cause impacto no tráfego da rede e esteja, sempre, apoiado na ciência e autorização do supervisor imediato do colaborador.

As seguintes atividades, sem exceção, são estritamente proibidas:

a) Envio de mensagens de e-mail não solicitadas, incluindo o envio de "correspondências indesejadas", ou outro material publicitário para pessoas que não solicitaram especificamente esse material (e-mail de spam).

b) Qualquer forma de assédio por e-mail, telefone ou mensagem de texto, seja pela linguagem, frequência ou tamanho das mensagens.

c) Uso não autorizado ou falsificação de informações do cabeçalho dos e-mails.

d) Solicitação de e-mail para qualquer outro endereço de e-mail, que não seja o da conta do autor da publicação, com a intenção de assediar ou extrair respostas.

e) Criação ou encaminhamento de "correntes", "pirâmide financeira" ou outros esquemas de "pirâmide" de qualquer tipo.

f) Uso de e-mails não solicitados originados das redes do “Intex Bank” ou outros provedores de serviços que atuam ou anunciam em nome da empresa, qualquer serviço hospedado pelo “Intex Bank” ou conectado por meio da rede do “Intex Bank”.

10. Referências

A equipe é responsável por ler e cumprir todas as políticas relevantes às suas funções e responsabilidades.

Função	Propósito
Política de Controle de Acesso	Limitar o acesso a informações e sistemas de processamento de informações, redes e instalações a partes autorizadas, de acordo com os objetivos comerciais.
Política de Gestão de Ativos	Identificar os ativos da organização e definir as responsabilidades de proteção adequadas.
Plano de Continuidade de Negócios e Recuperação de Desastres	Preparar o "Intex Bank" para o caso de interrupções prolongadas de serviço causadas por fatores fora de nosso controle (por exemplo, desastres naturais, eventos causados pelo homem) e para restaurar os serviços da forma mais ampla possível em um prazo mínimo.
Política de Criptografia	Garantir o uso adequado e eficaz da criptografia para proteger a confidencialidade, a autenticidade e/ou a integridade das informações.
Política de Classificação de Informação	Garantir a classificação e proteção das informações de acordo com a importância delas para a organização.
Política de Recursos Humanos	Garantir que funcionários e prestadores de serviços atendam aos requisitos de segurança, entendam suas responsabilidades e sejam adequados para suas funções.
Plano de Resposta a Incidentes	Política e procedimentos para incidentes de segurança da informação suspeitos ou confirmados.
Política de Segurança das Operações	Garantir a operação correta e segura dos sistemas e instalações de processamento de informações.
Política de Segurança Física	Evitar o acesso físico não autorizado ou danos às informações e às instalações de processamento de informações da organização.
Política de Gestão de Riscos	Definir o processo de avaliação e gerenciamento dos riscos de segurança da informação do "Intex Bank" para atingir os objetivos comerciais e de segurança da informação da empresa.
Política de Desenvolvimento Seguro	Garantir que a segurança das informações seja concebida e implementada durante o desenvolvimento dos aplicativos e sistemas da informação.
Política de Gerenciamento de Terceiros	Garantir a proteção dos dados e ativos da organização que são compartilhados, acessíveis ou gerenciados por fornecedores, incluindo partes externas ou organizações terceirizadas, como prestadores de serviços, vendedores e clientes; e manter um nível acordado de segurança de informações e prestação de serviços de acordo com os contratos com fornecedores.
Política de Cibersegurança	Definir diretrizes específicas para a proteção cibernética da empresa, com foco na defesa de ativos digitais, prevenção e resposta a ameaças cibernéticas.

11. Disposições Finais

O "Intex Bank" medirá e verificará a conformidade com esta política por meio de vários métodos, incluindo, entre outros, o monitoramento contínuo e auditorias internas e externas.

Assim como a ética, a segurança da informação, também, deve ser entendida como parte fundamental da cultura interna do “Intex Bank”, ou seja, qualquer incidente de segurança será considerado e tratado como se fosse e, como de fato é, um agente atuando contra a ética e os bons costumes regidos pela instituição no intuito de mitigar riscos e evitar possíveis incidentes.

Em casos de dúvidas ou esclarecimentos sobre o conteúdo desta política, ou sobre a aplicação do mesmo em relação a algum assunto específico, o colaborador do “Intex Bank” deverá entrar em contato a qualquer momento com o Gestor de Tecnologia da Informação.

12. Exceções

Exceções a esta política devem ser formalmente submetidas ao Gestor de Tecnologia da Informação 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.

13. Violações e Não Cumprimento da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente ao Gestor de TI 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.

14. 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.