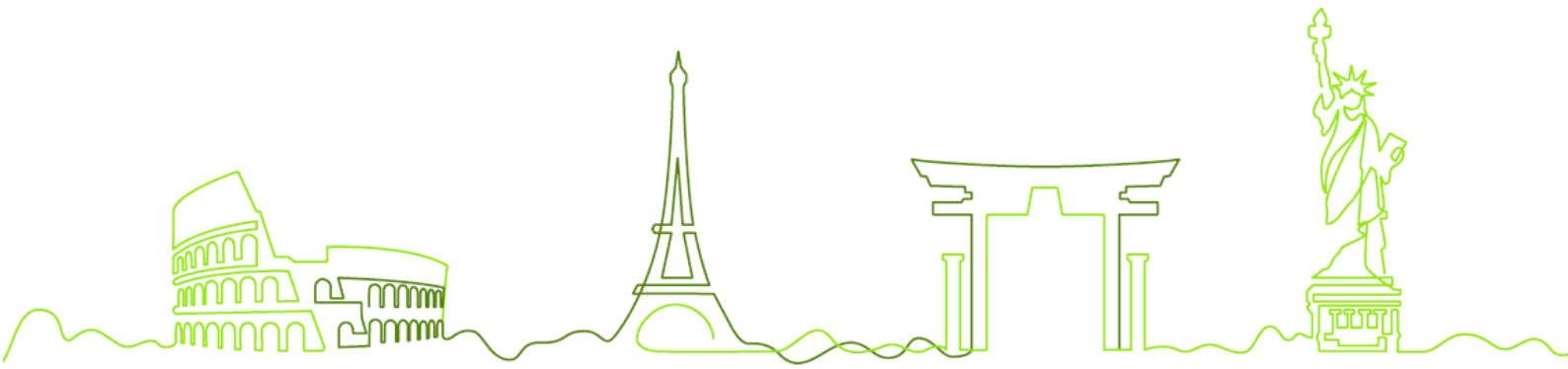

Política de Segurança Física

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	30/11/2024	Cibersegurança / T.I	Versão Original

Sumário

1. Objetivo

Esta política visa estabelecer diretrizes para garantir a proteção física de pessoas, informações, instalações, equipamentos e ativos do Intex Bank Banco de Câmbio S/A, referenciada abaixo somente como “Intex Bank”, contra ameaças como acesso não autorizado, furtos, roubos, danos e interrupções operacionais. Além de também objetivar a mitigação de riscos à segurança, proteger os dados sensíveis dos clientes e garantir o cumprimento das normas e regulamentações vigentes.

2. Escopo

Esta política se aplica a todos os funcionários do “Intex Bank” e a todas as partes externas com acesso físico às instalações próprias ou alugadas do “Intex Bank”.

Esta Política está alinhada com a Resolução CMN nº 4.893/2021 e a Resolução BCB nº 85/2021, que exigem a adoção de medidas físicas e lógicas de segurança para proteção dos ambientes críticos e para a gestão eficaz dos riscos operacionais. Além disso, incorpora boas práticas do NIST Cybersecurity Framework (CSF) e da ISO/IEC 27001:2022, particularmente no que se refere ao controle de acesso físico, proteção ambiental e segurança de instalações de processamento de dados. A política também reforça a aderência à LGPD (Lei nº 13.709/2018), ao mitigar riscos relacionados ao acesso não autorizado a dados pessoais armazenados fisicamente, e está alinhada com as exigências da Lei nº 9.613/1998, ao prevenir a utilização indevida de instalações e sistemas em atividades relacionadas à lavagem de dinheiro.

3. Perímetro de Segurança Física

Os escritórios físicos e as instalações de processamento devem atender a todos os códigos de construção locais referentes a materiais de construção de paredes, janelas, portas e mecanismos de controle de acesso. Algumas zonas internas podem ser identificadas como áreas seguras/ restritas, onde o acesso físico é restrito a um subconjunto de funcionários do “Intex Bank”, como escritórios particulares, armários de fiação, racks de servidores e salas de impressão e servidores.

4. Controles de Acesso Físico

As áreas seguras devem ser protegidas por controles de entrada apropriados para que somente o pessoal autorizado tenha permissão de acesso. Sempre que possível, os sistemas de controle de acesso do “Intex Bank” devem estar vinculados a um sistema

centralizado que fornece controle de acesso granular para funcionários. Os eventos de acesso devem ser registrados adequadamente e revisados conforme necessário, de acordo com o risco. Todas as áreas de acesso público, assim como as áreas restritas, serão monitoradas 24 horas por dia por câmeras de segurança, com gravações armazenadas por pelo menos 90 dias, onde o acesso ao sistema de monitoramento é restrito a profissionais de segurança designados e a gravação estará disponível para consulta em caso de incidentes.

A manutenção de equipamentos de segurança, como portas automáticas, cofres e câmeras, deve ser feita periodicamente para garantir o funcionamento adequado, e somente por pessoal estritamente autorizado e capacitado.

O processo para a concessão de acesso para as instalações, através dos crachás, deve incluir a aprovação da área de Tecnologia da Informação, além disso a área deve revisar os direitos de acesso dos colaboradores, com o objetivo de remover o acesso de qualquer parte que já não necessite mais do mesmo, como indivíduos que mudem de cargo dentro da organização ou que sejam afastados de suas atividades.

Os crachás de acesso não devem ser compartilhados ou emprestados a qualquer outra pessoa. No caso de perda ou roubo, eles devem ser relatados para a área de Tecnologia da Informação, ainda, os crachás que não forem mais necessários devem ser devolvidos para a área de Tecnologia da Informação. Eles não devem ser realocados para outros indivíduos ignorando o processo formal de devolução.

5. Proteção de Escritórios, Salas e Instalações

A segurança física de escritórios, salas e instalações deve ser projetada e implementada para proteger contra roubo, uso indevido, ameaças ambientais, acesso não autorizado e outras ameaças à confidencialidade, integridade e disponibilidade de dados e sistemas classificados.

A manutenção das dependências físicas do “Intex Bank” será realizada por pessoal previamente autorizado. O monitoramento deste ambiente deve ser realizado em tempo integral.

5.1. Proteção Contra Ameaças Ambientais e Externas

Uma proteção física contra desastres naturais, ataques maliciosos ou acidentes deve ser projetada e implementada. As áreas seguras devem ser monitoradas por meio de controles apropriados, como sistemas de detecção de intrusão, alarmes e/ou sistemas de vigilância por vídeo, quando possível. O acesso de visitantes e de terceiros às áreas

seguras deve ser restrito para reduzir o risco de perda e roubo de informações.

As instalações de processamento da produção devem ser equipadas com controles adequados ambientais e de continuidade de negócios, como sistemas de supressão de incêndio, sistemas de controle e monitoramento climático e sistemas de energia de reserva de emergência. O hardware do sistema de informações físicas e a infraestrutura de suporte devem passar por revisão e manutenção regulares de acordo com as recomendações do fabricante.

Cabos de energia, assim como cabos de rede, não devem estar presentes em locais que coloquem em risco a infraestrutura e a informação. Dá-se como exemplo a proximidade de conexões elétricas em ambientes que podem gerar curtos-circuitos ou a existência de cabos de rede em ambientes onde pessoas não autorizadas possam ter acesso e, consequentemente, acessar também a rede de dados, além disso os cabos de energia devem ser segregados dos cabos de comunicação, para evitar interferências.

O “Intex Bank” considera o fornecimento de energia elétrica como serviço crítico para suas atividades. Por essa razão, no endereço sede, o “Intex Bank” dispõe de equipamentos de nobreak, para os servidores, o qual é acionado automaticamente no caso de interrupção no fornecimento de energia.

5.2. Datacenter

5.2.1 Local

O acesso ao Datacenter Local é restrito a pessoas previamente autorizadas pela Gerência de Tecnologia da Informação. O controle de acesso é realizado por meio de fechadura eletrônica e o registro de acessos devem ser monitorados e auditados periodicamente para garantir a segurança do ambiente.

5.2.2 Terceirizado

O Datacenter terceirizado opera totalmente em nuvem e está sob a gestão da empresa RTM Infraestrutura em Tecnologia da informação Ltda, que implementa e mantém padrões rigorosos de segurança física, conforme descrito abaixo:

a) Proteção de perímetros físicos: Áreas críticas são cercadas e monitoradas para evitar acessos não autorizados;
b) Controle de acesso a ambientes físicos: Sistemas de autenticação e vigilância restringem o acesso às instalações físicas somente a pessoal autorizado;
c) Proteção contra desastres naturais: Infraestruturas são projetadas para resistir a riscos como enchentes, incêndios e terremotos, garantindo a

continuidade do serviço;

d) Gestão de áreas de entrega e carregamento: Procedimentos específicos garantem a segurança durante a entrada e saída de materiais, reduzindo riscos de violação ou comprometimento do ambiente físico.

6. Áreas de Entrega e Carga

Os pontos de acesso, como áreas de entrega e carga e outros pontos em que pessoas não autorizadas possam entrar em áreas seguras, devem ser controlados e, se possível, isolados das instalações de processamento de informações para evitar o acesso não autorizado.

7. Trabalho em Áreas Seguras e Gestão de Visitantes

O acesso dos visitantes aos escritórios somente é permitido mediante identificação com registro em foto e apresentação de documento de identidade válido, na recepção localizada no piso térreo. O acesso aos escritórios somente é liberado após autorização do "Intex Bank" (condômino), munido de crachá eletrônico que permite acesso exclusivo aos elevadores.

Não será permitido o acesso de visitantes, entregadores, técnicos de apoio externos e outros agentes externos a áreas seguras sem escolta e/ou supervisão adequada, além disso, funcionários que não necessitam acessar determinadas áreas por suas funções devem ser limitados a essas áreas.

Não serão permitidos em áreas seguras de acesso restrito o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis ou similares, caso seja necessário o mesmo deve ocorrer somente com autorização prévia do Departamento de Tecnologia da Informação.

Terceiros em áreas seguras devem documentar a entrada e saída em um registro de visitantes e serão escoltados ou monitorados pelos colaboradores do "Intex Bank". O funcionário do "Intex Bank" que identificar visitantes desacompanhados deve se aproximar do visitante, confirmar sua situação e garantir que ele retorne às áreas aprovadas ou informar essa ocorrência à autoridade responsável, conforme necessário.

O acesso de terceiros a áreas seguras deve ser confirmado com o responsável adequado do "Intex Bank" antes que o acesso seja concedido. Os colaboradores do "Intex Bank" que fornecem acesso a terceiros em áreas seguras são responsáveis por garantir que o pessoal externo cumpra todos os requisitos de segurança e seja responsável por todas

as ações tomadas por pessoas externas à que fornecem acesso. Os visitantes podem ser autorizados a trabalhar desacompanhados, desde que a parte responsável do "Intex Bank" possa garantir que eles não terão acesso não autorizado aos sistemas de informação, redes ou dados do "Intex Bank".

Visando a segregação de funções e o combate ao conflito de interesse, as salas das equipes de Cadastro, Análises de Clientes, Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e, Tecnologia e Segurança da Informação, têm acesso restrito permitido somente aos funcionários e colaboradores de cada departamento mediante senha em dispositivo eletrônico para acionamento de trava eletromagnética. As senhas são alteradas a cada 90 dias, não podendo serem repetidas as últimas duas (2) senhas anteriormente utilizadas.

8. Segurança de Fornecedores e Terceiros

Fornecedores e terceiros devem cumprir os requisitos de segurança física e os controles ambientais do "Intex Bank". O "Intex Bank" deve avaliar a adequação dos controles de segurança física de terceiros como parte do processo de gestão de fornecedores, de acordo com a Política de Gestão de Terceiros.

9. Exceções

Exceções a esta política devem ser submetidas formalmente ao Gestor de Tecnologia da Informação e Encarregado de Proteção de Dados para avaliação e aprovação, assegurando que cada caso seja documentado e justificado.

10. Violações e Não Cumprimento da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente ao Gestor de Tecnologia da Informação 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.

11. 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.

Intex Bank Banco de Câmbio S/A