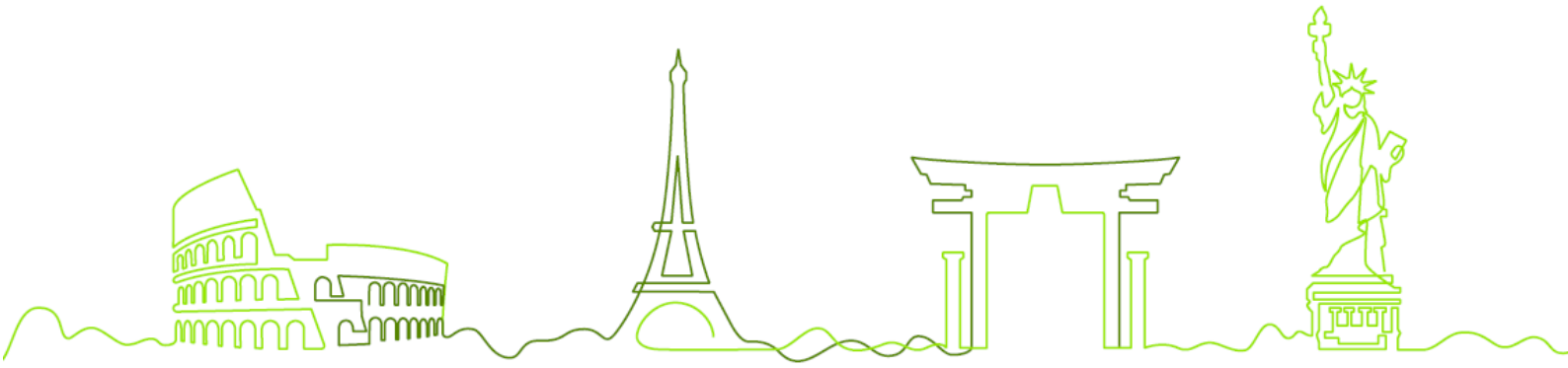

Política de Controle de Acesso

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	28/02/2025	Cibersegurança / T.I	Versão Original

Sumário

1. Objetivo

Esta política tem o objetivo de delimitar o acesso a informações e sistemas de processamento de informações, redes e instalações a partes autorizadas, de acordo com os objetivos comerciais do Intex Bank Banco de Câmbio S/A, referenciado abaixo somente como “Intex Bank”.

2. Escopo

Todos os sistemas de informação do “Intex Bank”, que processam, armazenam e transmitem dados confidenciais, conforme definido na Política de Classificação de Informação do “Intex Bank”. Esta política se aplica a todos os colaboradores e a todas as partes externas com acesso a redes e recursos do sistema do “Intex Bank”.

Esta política está alinhada com as diretrizes da Resolução CMN nº 4.893/2021 e da Resolução BCB nº 85/2021, que estabelecem requisitos para a estrutura de segurança cibernética e controles de acesso em instituições autorizadas pelo Banco Central do Brasil, bem como a gestão de incidentes e a proteção da infraestrutura crítica. Adota ainda boas práticas internacionalmente reconhecidas, como o NIST Cybersecurity Framework (CSF), referência para gestão de riscos e segurança cibernética, e a ISO/IEC 27001:2022, padrão que orienta a implementação de controles técnicos e administrativos em sistemas de gestão de segurança da informação (SGSI). A política também reforça o compromisso do “Intex Bank” com a LGPD (Lei nº 13.709/2018), especialmente no que se refere ao tratamento seguro de dados pessoais, e com a Lei nº 9.613/1998, garantindo controles eficazes para a prevenção à lavagem de dinheiro, por meio da restrição de acessos e do monitoramento contínuo das operações.

3. Política

O acesso aos recursos de computação da informação é limitado ao pessoal com requisitos comerciais para tal acesso. Os direitos de acesso serão concedidos ou revogados de acordo com esta política pela equipe de Tecnologia da Informação, mediante aprovação formal.

3.1 Controle de Acesso

O “Intex Bank” determinará o tipo e nível de acesso concedido a usuários com base no “princípio do menor privilégio”. Esse princípio afirma que os usuários recebem apenas o nível de acesso absolutamente necessário para desempenhar suas funções e é estabelecido pelos requisitos comerciais e de segurança do “Intex Bank”. As permissões e os direitos de acesso não expressamente concedidos devem ser proibidos por padrão.

O principal método do “Intex Bank” para atribuir e manter controles de acesso e direitos de acesso consistentes deve ser a implementação do controle de acesso baseado em função (RBAC). Sempre que possível, os direitos e as restrições devem ser alocados a grupos. As contas de usuários individuais podem receber permissões adicionais, conforme necessário, com a aprovação do proprietário do sistema ou da parte autorizada.

Todos os acessos privilegiados à infraestrutura de produção devem utilizar

autenticação multifatorial (MFA).

3.2 Acesso a Redes e Serviços de Rede

A fim de detectar e proteger a rede contra acesso não autorizado e, ao mesmo tempo, fornece acesso imediato a usuários legítimos, os acessos aos serviços de rede internos e externos devem ser controlados, devido a isso os seguintes padrões de segurança regem o acesso às redes e aos serviços de rede do "Intex Bank":

a. O acesso técnico às redes do "Intex Bank" deve ser formalmente documentado, incluindo a função padrão ou o aprovador, o outorgante e a data.
b. Somente funcionários autorizados do "Intex Bank" e terceiros com contrato assinado ou declaração de trabalho, que tenham necessidade comercial, terão acesso às redes e recursos de produção.
c. O acesso à rede de convidados será concedido mediante registro na recepção, com identificação do convidado e do funcionário responsável pelo acompanhamento. A rede de convidados deve ser segregada da rede corporativa, garantindo que os convidados tenham acesso limitado à internet e não acessem recursos internos.
d. Conexões remotas a sistemas e redes de produção devem ser obrigatoriamente criptografadas e protegidas por VPN, onde os parâmetros de segurança para configuração de VPN devem ser definidos pela área de TI da "Intex Bank".
e. As boas práticas de uso e acesso às redes estão detalhadas na Política de Segurança da Informação da "Intex Bank", que deve ser do conhecimento de todos os usuários.

3.3 Gerenciamento de Acesso do Cliente

Ao configurar o acesso entre contas usando funções do Portal, se deve usar um valor gerado para o ID externo, em vez de um valor fornecido pelo cliente, para garantir a integridade da configuração da função entre contas. Um ID externo gerado por um parceiro garante que partes mal-intencionadas não possam imitar a configuração de um cliente e reforça a exclusividade e a consistência do formato em todos os clientes.

Os IDs externos usados devem ser exclusivos para todos os clientes. A reutilização de IDs externos para clientes diferentes não resolve o problema de ambiguidade de representação e corre o risco de que o cliente A possa ver os dados do cliente B usando a função ARN do cliente B junto com o ID externo do cliente B.

Os clientes não devem ser capazes de definir ou influenciar IDs externos. Quando o ID externo é editável, é possível que um cliente represente a configuração de outro.

3.4 Gerenciamento de Acesso do Usuário

O "Intex Bank" requer que todo o pessoal tenha um identificador de usuário exclusivo, previamente definidos pela TI, para acesso ao sistema e que as credenciais e senhas do usuário não sejam compartilhadas entre vários funcionários. Os usuários com vários níveis de acesso (por exemplo, administradores), sempre que possível, devem receber contas separadas para utilização normal do sistema e para funções administrativas. As contas raiz, de serviço e de administrador podem usar um sistema de gestão de senhas para compartilhar senhas apenas para fins de continuidade de negócios. Os administradores só devem usar contas administrativas compartilhadas conforme

necessário. Se uma senha for comprometida ou suspeita de comprometimento, o incidente deve ser encaminhado para TI imediatamente e a senha deve ser alterada.

3.4.1 Registro e Cancelamento de Registro de Usuários

Somente a área de Tecnologia da Informação poderá criar IDs de usuário e só poderão fazê-lo mediante o recebimento de uma solicitação documentada de partes autorizadas (RH ou Gestor de Área). As solicitações de provisionamento de usuários devem incluir a aprovação dos proprietários dos dados ou da gerência do "Intex Bank" autorizada a conceder acesso ao sistema. Antes da criação da conta, os administradores devem verificar se a conta não viola nenhuma política de segurança ou de controle de acesso ao sistema do "Intex Bank", como segregação de deveres, medidas de prevenção contra fraudes ou restrições de direitos de acesso.

Os IDs de usuário devem ser prontamente desativados ou removidos quando os usuários deixarem a organização ou quando o contrato de trabalho terminar, de acordo com os SLAs. Os IDs de usuário não devem ser reutilizados.

3.4.2 Provisionamento de Acesso do Usuário

a) Os novos funcionários e/ou contratados não devem ter acesso a nenhum sistema de produção do "Intex Bank" até que tenham concluído todas as tarefas de integração de RH, que podem incluir, entre outras, contrato de trabalho assinado, contrato de propriedade intelectual e reconhecimento das políticas de segurança da informação do "Intex Bank".
b) O acesso deve ser restrito apenas ao que é necessário para realizar as tarefas do trabalho.
c) Nenhum acesso pode ser concedido antes da data oficial de início do funcionário.
d) As solicitações de acesso e as modificações de direitos devem ser documentadas em um tíquete ou e-mail de solicitação de acesso. Nenhuma permissão deve ser concedida sem a aprovação do proprietário ou da gerência do sistema ou dos dados.
e) Os registros de todas as alterações de permissões e privilégios devem ser mantidos por, no mínimo, um ano.

3.4.3 Avaliação de Acesso do Usuário

Os administradores devem realizar revisões dos direitos de acesso das contas de usuários, administradores e de serviços, **trimestralmente** para verificar se o acesso do usuário está limitado aos sistemas necessários para sua função de trabalho. As revisões de acesso devem ser devidamente documentadas e devem seguir o processo estabelecido pelo fluxo de liberação e revisão de acessos, presente no anexo 1.

As avaliações de acesso podem incluir participação em grupos, bem como avaliações de qualquer permissão específica ou baseada em exceções. Os direitos de acesso também devem ser revisados como parte de uma mudança de função, incluindo promoção, rebaixamento ou transferência dentro da empresa.

3.5 Gerenciamento de Acesso Priveligiado

O “Intex Bank” deve garantir que a alocação e o uso de direitos de acesso privilegiados sejam restritos e gerenciados criteriosamente. O objetivo é garantir que somente usuários, componentes de software e serviços autorizados recebam direitos de acesso privilegiado. O “Intex Bank” garantirá que o acesso e os privilégios estejam em conformidade com o seguinte padrão:

a. Identificar e validar usuários: identifique os usuários que precisam de acesso privilegiado para cada sistema e processo.
b. Atribuir direitos privilegiados: conceda direitos de acesso baseando as alocações em necessidades e competências específicas e aderindo estritamente à esta política.
c. Manter protocolos de autorização: mantenha registros de todas as alocações de acesso privilegiado.
d. Impor uma autenticação forte: exija MFA para todos os acessos privilegiados.
e. Impedir o uso de IDs administrativos genéricos: impeça o uso de IDs de usuários administrativos genéricos.
f. Adotar protocolos de acesso com limite de tempo: conceda acesso privilegiado apenas pelo tempo necessário para realizar tarefas específicas e revogue-o assim que a tarefa for concluída.
g. Garantir o registro e a auditoria: registre todos os logins e atividades privilegiadas.

3.6 Revogação e Ajuste de Direitos de Acesso

Os direitos de acesso de todos os usuários devem ser prontamente removidos após a rescisão de seu emprego ou contrato, ou quando os direitos não forem mais necessários devido a uma mudança na função ou no cargo. O período máximo permitido para a rescisão do acesso é 24 horas.

3.7 Procedimento de Acesso a Provisionamento, Desprovisionamento e Alterações

Ao término do processo de integração, o RH preencherá um formulário, onde emitirá um alerta para TI, onde ela fornecerá acesso a todos os sistemas de toda a empresa, bem como aos sistemas de engenharia para o grupo de Membros da Equipe Técnica (MTS). O acesso adicional, além do acesso padrão pré-aprovado, deve ser solicitado e aprovado por um gerente ou proprietário do sistema.

3.8 Separação de Responsabilidades

Deveres e responsabilidades conflitantes devem ser segregados para reduzir o risco de modificação ou uso indevido não autorizado ou não intencional dos ativos do “Intex Bank”. Ao provisionar o acesso, preste a devida atenção para que nenhuma pessoa possa acessar, modificar ou usar os ativos sem autorização ou detecção. O início de um evento deve ser separado de sua autorização. A possibilidade de conluio deve ser considerada ao determinar os níveis de acesso para indivíduos e grupos.

3.9 Responsabilidade do Usuário pelo Gerenciamento de Credenciais de Autenticação

O controle e o gerenciamento de senhas de usuários individuais são de responsabilidade de todo o pessoal do "Intex Bank"e de usuários externos. Os usuários devem proteger as informações secretas de autenticação de acordo com as Políticas de Segurança da Informação.

4. Política de Senhas

4.1. Requisitos

a) Por padrão, as configurações descritas nesse documento, aplicam-se a todas as contas do domínio: "trevisocc.com.br", sistemas desenvolvidos pelo "Intex Bank" e dispositivos gerenciados pelo "Intex Bank" que não fazem autenticação no domínio seguem o mesmo padrão;
b) Sempre que um usuário for criado na estrutura "Intex Bank", a primeira senha deve ser alterada no primeiro login, sendo solicitada a troca automaticamente pelo sistema;
c) Sistemas de clientes, fornecedores e terceiros que não são de responsabilidade do "Intex Bank", devem adotar as melhores práticas visando a segurança de seus aplicativos e informações de seus clientes;
d) O "Intex Bank" adota as melhores práticas conforme padrão PCI-DSS.
   - A senha satisfaz os requisitos mínimos de complexidades, não sendo formada pelo nome da conta de usuário ou parte do nome da conta e possuindo caracteres entre letras minúsculas e maiúsculas, números e caracteres especiais; Comprimento mínimo de 8 caracteres;
   - Tempo de vida máximo de 90 dias;
   - As 3 últimas senhas não podem ser reutilizadas;
e) Para redefinições manuais de senha, a identidade do usuário deve ser verificada antes de alterar a senha;
f) Deve ser verificado por e-mail antes de uma solicitação de alteração de senha;
g) Exija a senha atual além da nova senha durante a alteração da senha;
h) Senhas devem ser armazenadas em formato 'hash' e 'salted' usando uma função de hash unidirecional que utilize memória ou CPU;
i) A senha e os ID´s são de uso pessoal e intransferível, a utilização por terceiros é passível de punições.

4.2. Bloqueio por Senha Incorreta

As senhas devem ser configuradas para serem bloqueadas após 5 tentativas fracassadas, caso a conta seja bloqueada não poderá ser utilizada até que o administrador faça o desbloqueio ou até que o tempo de bloqueio da conta seja expirado.

4.3. Recomendações e Cuidados

Recomenda-se não utilizar os itens descritos abaixo para a criação de uma senha "forte", já que podem ser obtidos com facilidade e utilizados na tentativa de quebra

de senha:

- Nomes ou sobrenomes.
- Número de documentos.
- Telefones.
- Placas de carro.
- Datas especiais.

Antes de digitar a senha tome os seguintes cuidados:

- Certifique-se que não está sendo observado.
- Não forneça sua senha a terceiros.
- Não utilizar a senha em computadores que não atendem os requisitos de segurança da empresa.
- Alterar a senha imediatamente se houver suspeita de que ela possa estar comprometida.

5. Acesso a sistemas e Aplicativos

5.1 Restrição de Acesso às Informações

Os aplicativos devem restringir o acesso às funções e às informações de programas aos usuários autorizados e ao pessoal de suporte, de acordo com esta política. O nível e o tipo de restrição aplicada por cada aplicativo devem ser baseados nos requisitos individuais do aplicativo, conforme definido pelo responsável pelos dados. A Política de Controle de Acessos específica do aplicativo também deve estar em conformidade com as políticas do "Intex Bank" referentes a controles de acesso e gerenciamento de dados.

Antes da implementação, critérios de avaliação devem ser aplicados ao software de aplicativo para determinar os controles de acesso e as políticas de dados necessários. Critérios de avaliação incluem, mas não estão limitados a:

a) Sensibilidade e classificação de dados.
b) Risco para a organização de acesso ou divulgação não autorizados de dados.
c) A capacidade e a granularidade de controle(s) de direitos de acesso do usuário ao aplicativo e aos dados armazenados no aplicativo.
d) Restrições nas saídas de dados, incluindo filtragem de informações confidenciais, controle de saída e restrição de acesso a informações a pessoal autorizado.
e) Controles sobre os direitos de acesso entre o aplicativo avaliado e outros aplicativos e sistemas.
f) Restrições programáticas ao acesso do usuário às funções do aplicativo e instruções privilegiadas.
g) Funcionalidade de registro e auditoria para funções de sistemas e acesso a informações.
h) Recursos de retenção e envelhecimento de dados.

Todas as contas padrão desnecessárias devem ser removidas ou desabilitadas antes de disponibilizar um sistema na rede. Especificamente, as senhas e credenciais padrão do fornecedor devem ser alteradas em todos os sistemas, dispositivos e infraestrutura do "Intex Bank" antes da implementação. Isso se aplica a TODAS

as senhas padrão, incluindo, mas não se limitando àquelas usadas por sistemas operacionais, software que fornece serviços de segurança, contas de aplicativos e sistemas e strings de comunidade SNMP (Simple Network Management Protocol), quando possível.

5.2 Procedimentos Seguros de Início de Sessão

Os controles de login seguro devem ser projetados e selecionados de acordo com a sensibilidade dos dados e o risco de acesso não autorizado com base na totalidade da arquitetura de segurança e controle de acesso.

5.3 Sistema de Gerenciamento de Senhas

Os sistemas de gerenciamento de senhas devem ser interativos e ajudar o pessoal do "Intex Bank" a manter padrões de senhas ao aplicar critérios de força de senha, incluindo comprimento mínimo e complexidade, quando possível.
Todo armazenamento e transmissão de senhas devem ser protegidos usando proteções criptográficas apropriadas, seja por meio de hash ou criptografia.

5.4 Uso de Programas Utilitários Privilegiados

O uso de programas utilitários, arquivos de sistema ou outro software que possa ignorar os controles do sistema e do aplicativo, ou alterar as configurações do sistema, deve ser restrito somente para pessoal autorizado. Os sistemas devem manter registros de todo o uso de utilitários do sistema ou alterações nas configurações do sistema. Utilitários de sistema divergentes ou outros programas privilegiados devem ser removidos ou desativados como parte do processo de construção e configuração do sistema.
A aprovação da gerência é necessária antes da instalação ou do uso de qualquer utilitário de sistema ad hoc ou de terceiros.

5.5 Acesso ao Código-Fonte do Programa

O acesso ao código-fonte do programa e aos itens associados, incluindo projetos, especificações, planos de verificação e planos de validação, deve ser estritamente controlado para impedir a introdução de funcionalidades não autorizadas no software, evitar alterações não intencionais e proteger a propriedade intelectual do "Intex Bank". Todo acesso ao código-fonte deve ser baseado nas necessidades da empresa e registrado para revisão e auditoria.

6. Exceções

As solicitações de exceção a esta política devem ser enviadas ao Gestor de Tecnologia da Informação para aprovação, e em casos de dúvidas, comentários ou necessidade de exceções, entre em contato pelo e-mail: suporte@intexbank.com.br.

7. Violações e Cumprimento da Política

Quaisquer violações conhecidas desta política devem ser informadas ao Gestor de Tecnologia da Informação. As violações desta política podem resultar na retirada ou

suspensão imediata dos privilégios do sistema e da rede e/ou em ações disciplinares de acordo com os procedimentos da empresa, até e inclusive a rescisão do contrato de trabalho.

8. 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 – Fluxo de Liberação e Revisão de Acessos