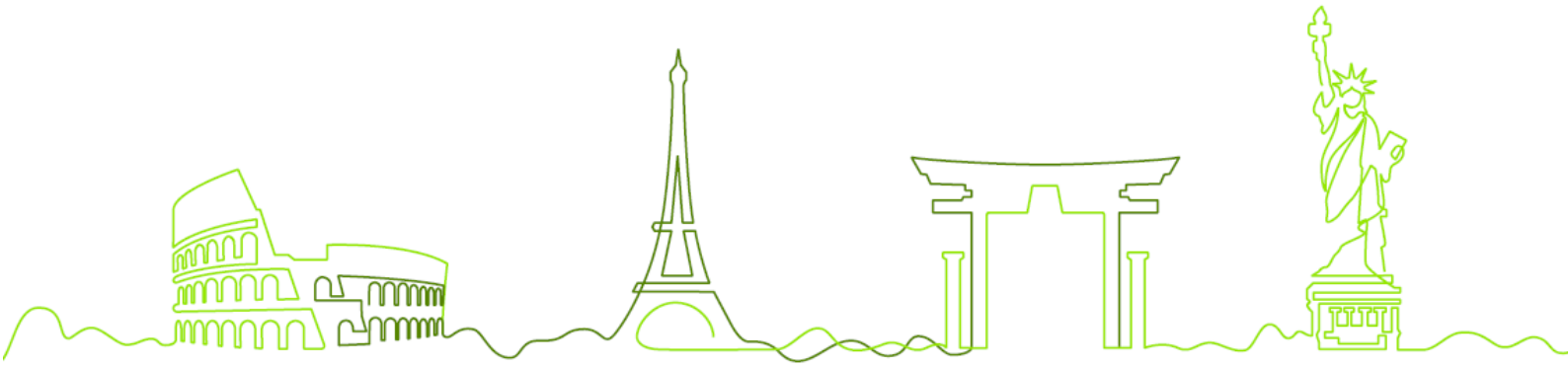

Política de Backup e Restore

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 como objetivo orientar os colaboradores da área de Tecnologia da Informação (TI) do "Intex Bank" sobre a importância dos backups e como realizá-los de forma eficiente e segura, garantindo a integridade e disponibilidade das informações em caso de incidentes.

Esta Política está alinhada com a Resolução CMN nº 5.088/2023, que estabelece diretrizes para a continuidade de negócios, segurança e riscos operacionais, impactando diretamente o planejamento de backup e recuperação (BCP/DRP). Além disso, reforça os princípios da Resolução CMN nº 4.893/2021 e da Resolução BCB nº 85/2021, que exigem estrutura robusta de segurança cibernética e gestão de riscos operacionais e de incidentes. Também adota boas práticas do NIST Cybersecurity Framework (CSF) e da ISO/IEC 27001:2022, especialmente no que se refere ao controle de integridade, proteção de dados e resiliência operacional.

Por fim, atende aos requisitos da LGPD (Lei nº 13.709/2018), assegurando a confidencialidade, a integridade e a disponibilidade dos dados pessoais tratados, e reforça o cumprimento da Lei nº 9.613/1998, ao contribuir para a prevenção à lavagem de dinheiro por meio da preservação e rastreabilidade das informações armazenadas.

2. Escopo

Esta política abrange os procedimentos de backup e restauração dos seguintes dados:

a) Arquivos de Rede (Servidor interno);
b) Banco de Dados;
c) Servidor de Aplicação.

3. Procedimento de Backup

3.1. Servidor de Arquivos

Os backups do servidor de arquivos são gerenciados pelo sistema Uranium, que realiza cópias de segurança automáticas de acordo com as regras definidas. O Gestor de TI deve verificar diariamente se os backups foram realizados corretamente, acessando o HD conectado ao data center.

- Rotação de HDs: São utilizados três HDs, que são alternados diariamente. O HD do backup mais recente é entregue ao diretor de correspondentes para armazenamento em cofre, e recolhido após um dia, em um ciclo contínuo.
- Armazenamento: Os HDs restantes devem ser armazenados na sala de TI, em local seguro e com acesso restrito ao Gestor e à diretoria.

Além desta política o procedimento para realização das cópias de seguranças, está definido no Anexo 1 – Fluxo de Backup e Restore.

3.2. Banco de Dados

O backup do banco de dados é realizado diariamente, diretamente no servidor em nuvem da RTM. Adicionalmente, é feito um snapshot de todo o sistema de aplicação.

3.3. Regras de Backup

A tabela a seguir exibe detalhes sobre os tipos de backups realizados:

Sistema	Tipo	Período	Retenção
Servidor de Arquivos	Completo	Diário (Segunda à Sexta – 18:00 as 06:00)	3 dias (HDs) e 30 dias (Logs do Uranium)
Banco de Dados	Completo	Diário (22:00 as 02:00)	1 dia

3.4. Procedimento de Backup Manual

O processo inicia com a verificação da conclusão do backup no servidor de arquivos, realizada pelo sistema **Uranium**. Ao detectar a finalização do backup, o sistema gera automaticamente um registro detalhado (log), contendo informações cruciais sobre o processo.

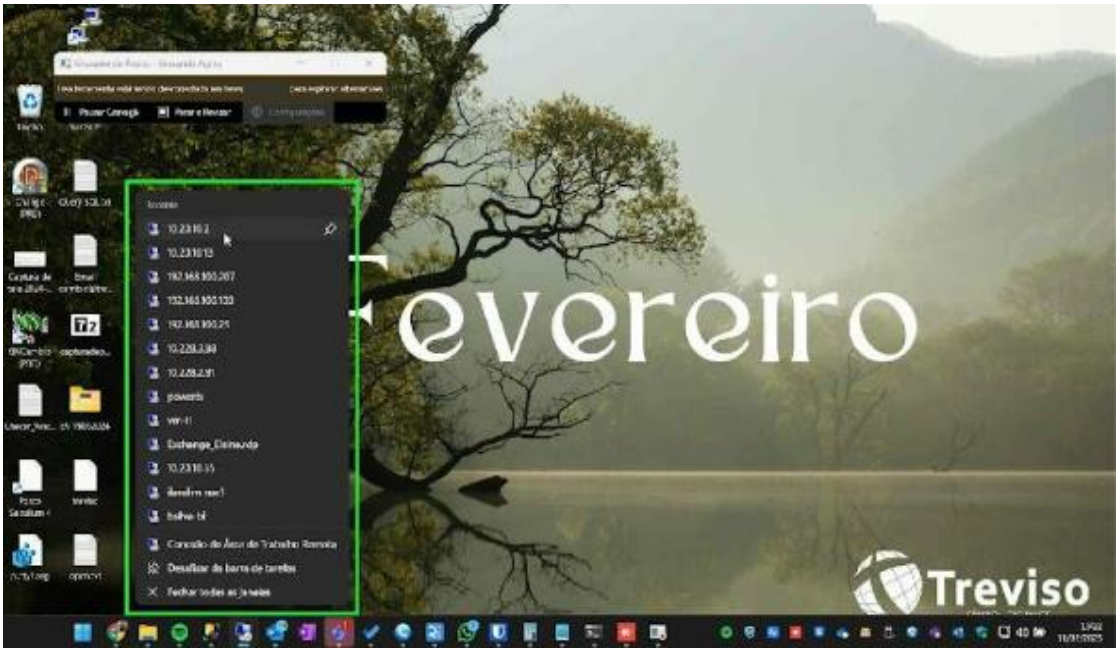

Figura 1 – Etapa 1: Acesso ao servidor de arquivos

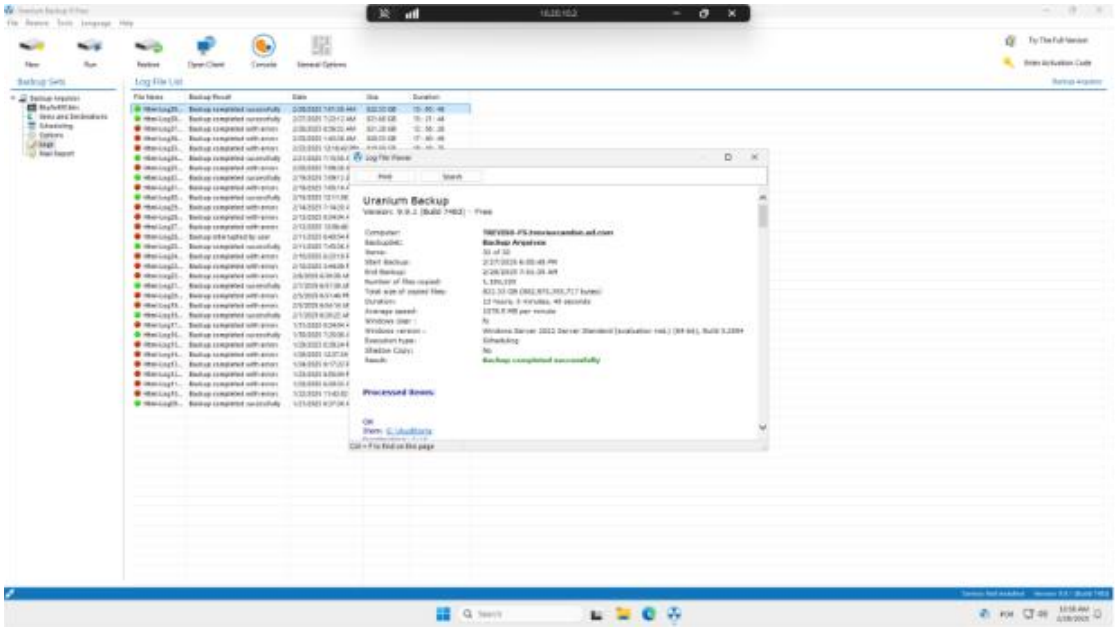

Figura 2 – Etapa 2: Verificação do log gerado pelo sistema Uranium

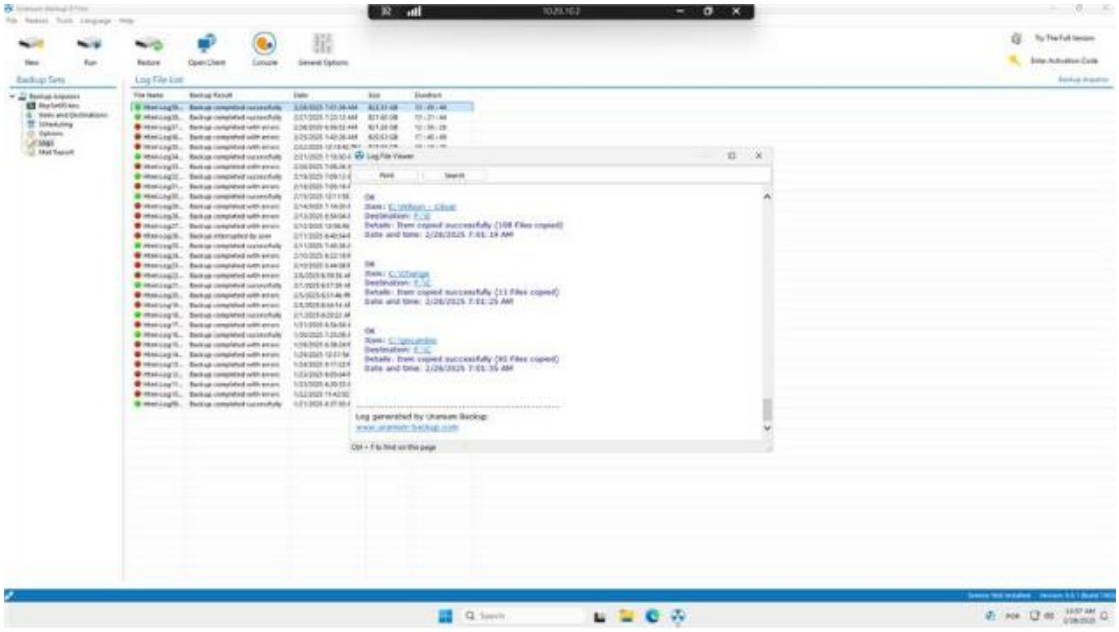

Figura 3 – Final do Log gerado pelo sistema Uranium

Concluído o backup, procede-se à remoção física do disco rígido do servidor (Etapa 3). Em seguida, realiza-se uma verificação de **três** arquivos aleatórios presentes no HD, assegurando a integridade e a completude do backup.

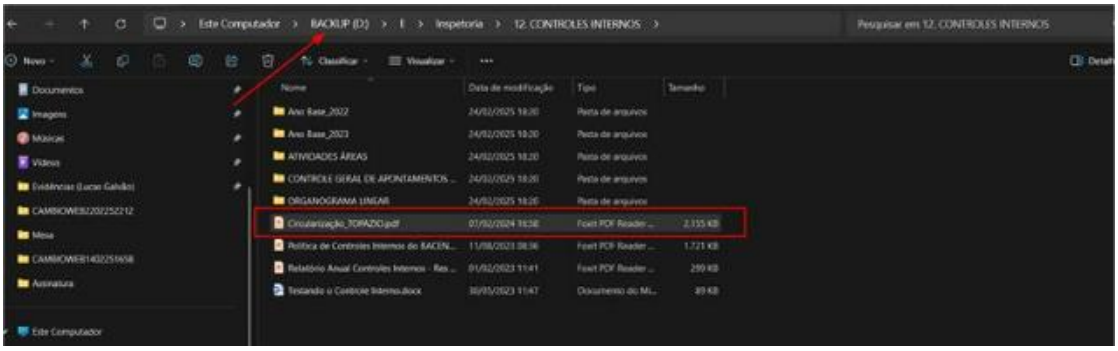

Figura 4 – Etapa 4: Verificação aleatória de arquivos (Arquivo 1)

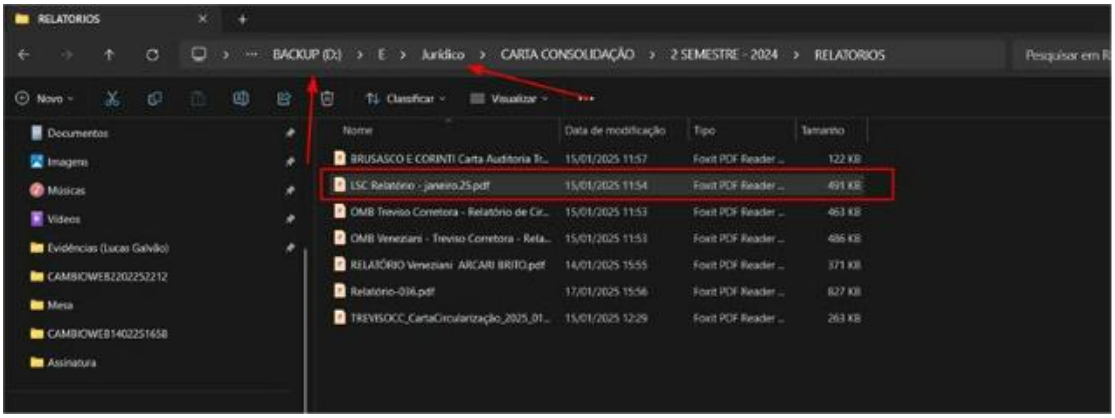

Figura 5 – Etapa 4: Verificação aleatória de arquivos (Arquivo 2)

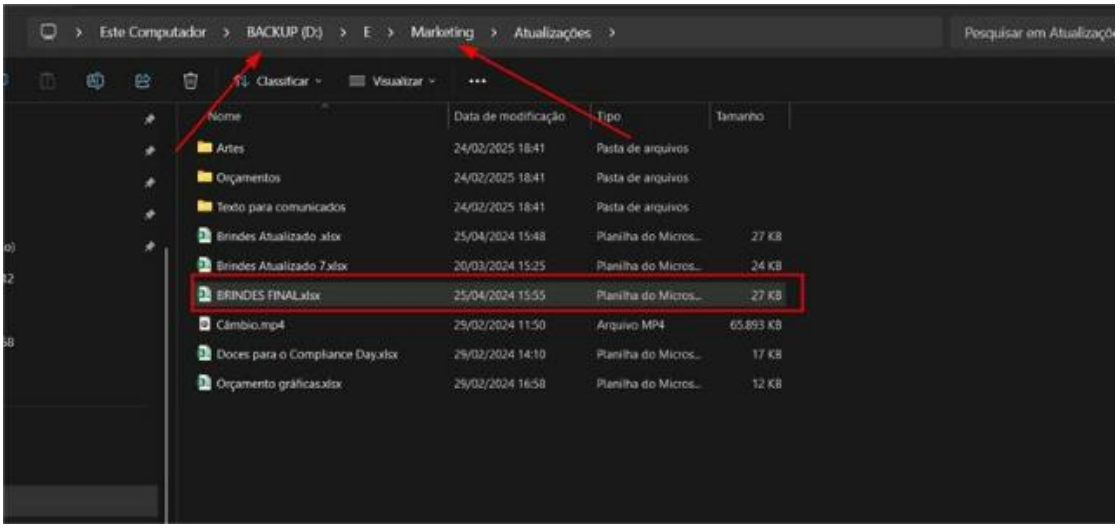

Figura 6 – Etapa 4: Verificação aleatória de arquivos (Arquivo 3)

Após a verificação dos arquivos no HD, ele deve ser entregue pessoalmente ao Diretor de Correspondentes, que o armazenará em um cofre dedicado (Etapa 5). Simultaneamente, o segundo HD, armazenado na Sala da TI, deve ser conectado ao servidor para garantir a continuidade das operações (Etapa 6). O terceiro HD, previamente armazenado no cofre da Diretoria, deve ser coletado e armazenado em local seguro e apropriado dentro da sala de TI, seguindo os protocolos de segurança da empresa (Etapa 7 e final).

3.5. Manuseio de Mídias

Somente pessoas autorizadas pelo “Intex Bank” podem manusear as mídias utilizadas para backup. Estas pessoas devem ser responsáveis pelas mídias e pelo zelo de todos os controles descritos nesta política e nas demais diretrizes do “Intex Bank” a fim de garantir o correto manuseio das mesmas.

Faz-se necessário um inventário de todas as mídias contendo cópias de segurança. Estas devem ser devidamente identificadas quanto ao seu conteúdo e data do backup. Possuir um rótulo que a identifique e diferencie das demais. A informação de que a mídia de backup é classificada como confidencial é obrigatória e deve estar presente no rótulo da mídia.

Toda mídia utilizada para backup deve ser classificada como confidencial - por isso, o conteúdo das mídias deve ser encriptado e o controle de acesso (físico e/ou lógico) à ferramenta de backup deve ser eficiente e revisado periodicamente. Com isso, garantindo que apenas as pessoas que necessitem deste acesso possuam permissão para fazê-lo.

3.6. Armazenamento de Mídias

As cópias de segurança são armazenadas em HDs com acesso restrito ao Gestor de TI e Diretoria.

O acesso físico aos dados copiados deve ser protegido contra destruição física e contra acessos não autorizados.

3.7. Transporte de Mídias

Caso seja necessário o transporte de mídias utilizadas para backup no “Intex Bank”, deve ser realizado de forma segura.

Para isso, faz-se necessário:

a) Proteger a(s) mídia(s) utilizando-se de um invólucro próprio para este fim que oculte o seu conteúdo interno e promova a preservação de sua integridade física de acordo com as recomendações do fabricante da mídia.

b) Possuir um adequado controle de saída da(s) mídia(s) do lugar de onde foi feito o backup, da(s) mídia(s) a ser(em) transportada(s) e da chegada desta(s) no site de armazenamento. O mesmo controle deve se aplicar quando o caminho for o inverso. Esta atividade deve ser realizada apenas quando formalmente autorizada pela Gestão de TI do “Intex Bank”.

c) Levar em consideração o risco de se efetuar o transporte em determinados lugares e/ou cidades considerados perigosos ou potencialmente perigosos. Sendo necessário efetuar o transporte em um local ou cidade considerado de alto risco, o nível de segurança que deve ser empregado no transporte precisa ser maior, devendo-se considerar a hipótese da contratação de uma empresa especializada para este fim ou outro controle que vise mitigar este risco a níveis aceitáveis pela organização.

Sempre que a responsabilidade desta atividade for terceirizada faz-se necessário o estabelecimento de um acordo de confidencialidade entre as partes.

3.8. Descarte de Mídias

O descarte das mídias utilizadas para backup deve ser realizado quando:

a) A mídia apresentar problemas;
b) A mídia for considerada imprópria, obsoleta ou fora dos parâmetros adotados pelo “Intex Bank”;
c) A mídia tiver o tempo de vida útil (de acordo com o fabricante da mesma) expirado.

Sempre que possível, antes de se efetuar o descarte, faz-se necessário efetuar uma tentativa de exclusão das informações constantes na fita através de formatação desta. Além disso, faz-se necessário efetuar um controle da(s) mídia(s) a ser(em) descartada(s) a fim de se manter um histórico desta atividade.

Assim como o transporte, esta atividade deve ser realizada apenas quando formalmente autorizada pela Gestão de TI do “Intex Bank”.

3.9. Testes das Cópias de Segurança

Testes de restauração são realizados após a conclusão dos backups para garantir a integridade das cópias. Os testes consistem na seleção aleatória de arquivos e restauração em um local diferente.

4. Restaurações de Informações

4.1. Procedimento de Restore

Testes de restauração são realizados para atualizar as bases de homologação dos sistemas (Change/E-guardian). O Gestor de TI deve avaliar o backup de homologação, acessar o SQL e verificar se o número de cadastro e operações estão de acordo com o ambiente de produção.

- **Frequência**: Conforme a necessidade.

4.1.1. Restore de Arquivos

Quando necessário restaurar um arquivo perdido, deve-se acessar a pasta de backup localizar o arquivo que deve ser copiado e colado em sua pasta de origem no sistema, garantindo sua correta restauração.

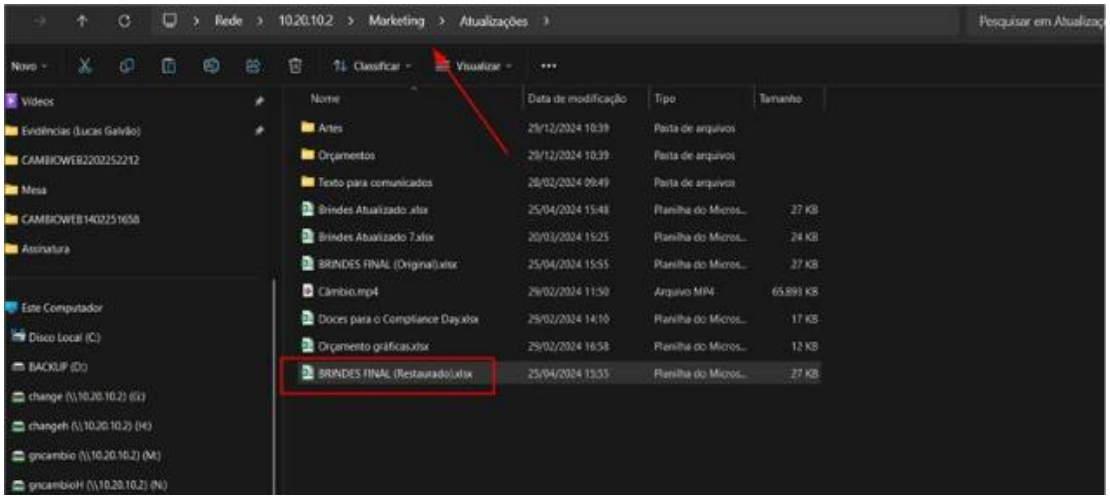

Figura 7 - Restauração de Arquivo para Rede

4.1.2. Restore de Banco de Dados

Quando necessário, deve ser aberto o SQL, onde deve ser acessado o backup de homologação e restaurá-lo, definindo o destino dos dados.

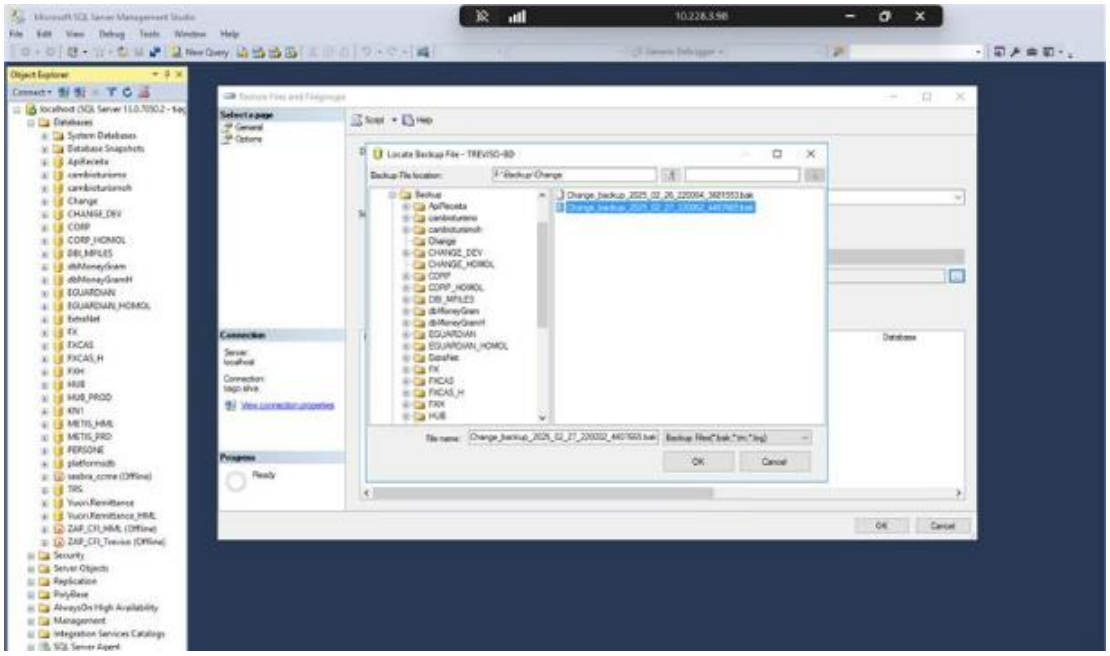

Figura 8 – Etapa 1: Seleção do Arquivo de Backup do Banco de Dados

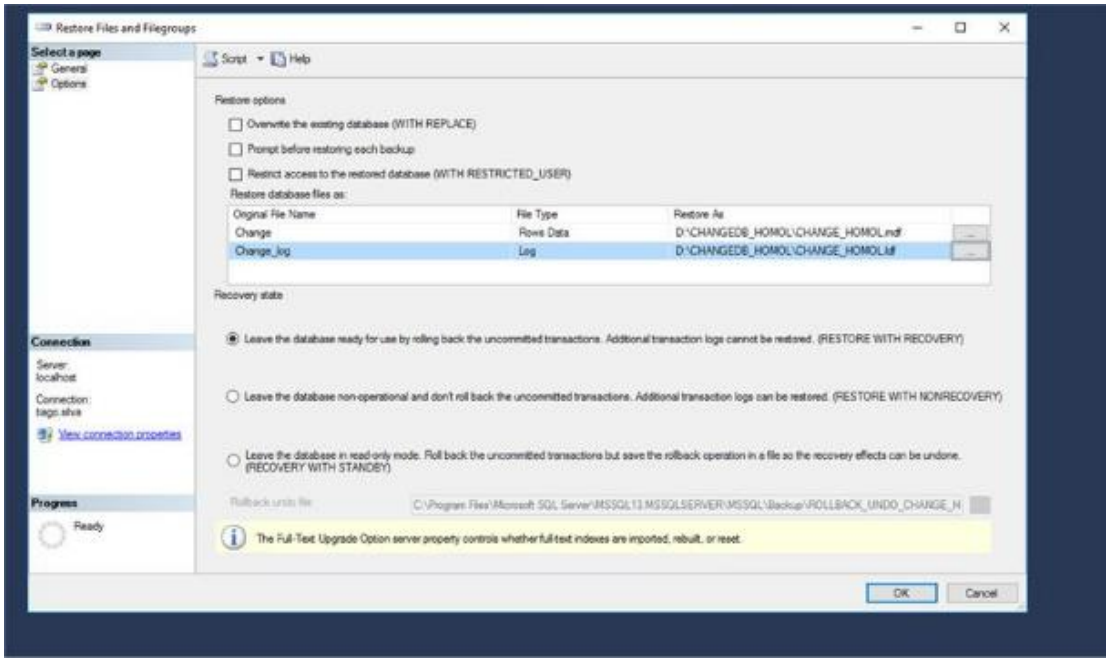

Figura 9 – Etapa 2: Apontamento para o destino dos dados do backup

- Após a seleção do destino dos dados, irá ser iniciado a restauração. Quando for finalizada, uma notificação aparecerá.

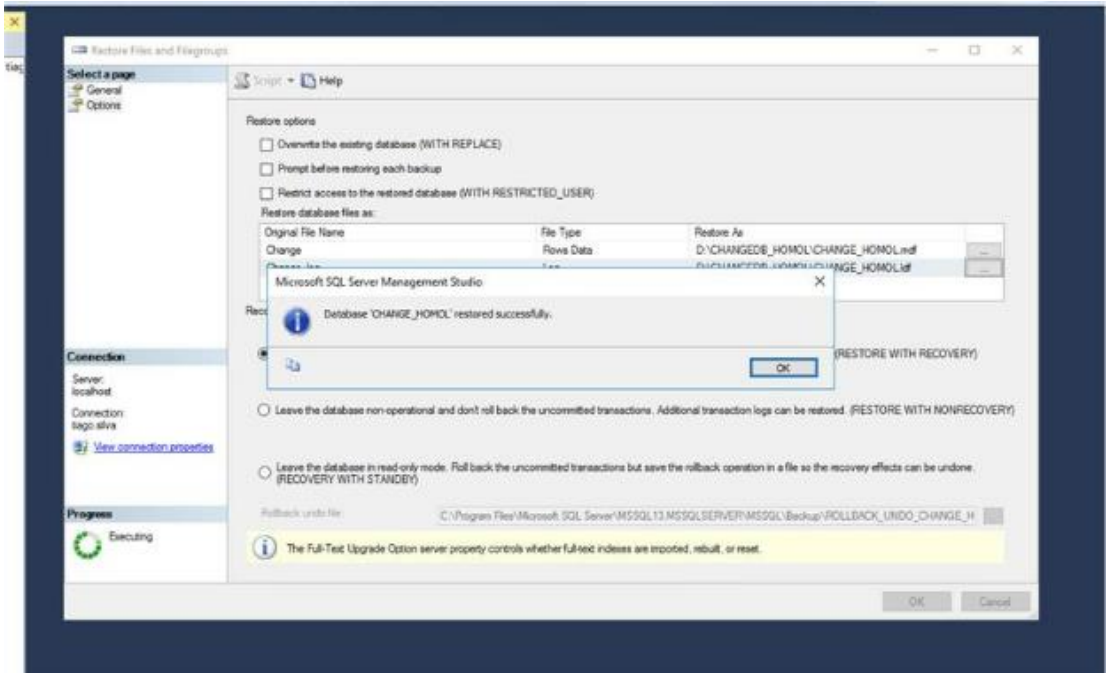

Figura 10 - Notificação de Finalização do Restore

Quando finalizada a restauração, deve ser verificado o restore em homologação, comparando os dados com o ambiente de produção, garantindo que não haja discrepâncias de informações.

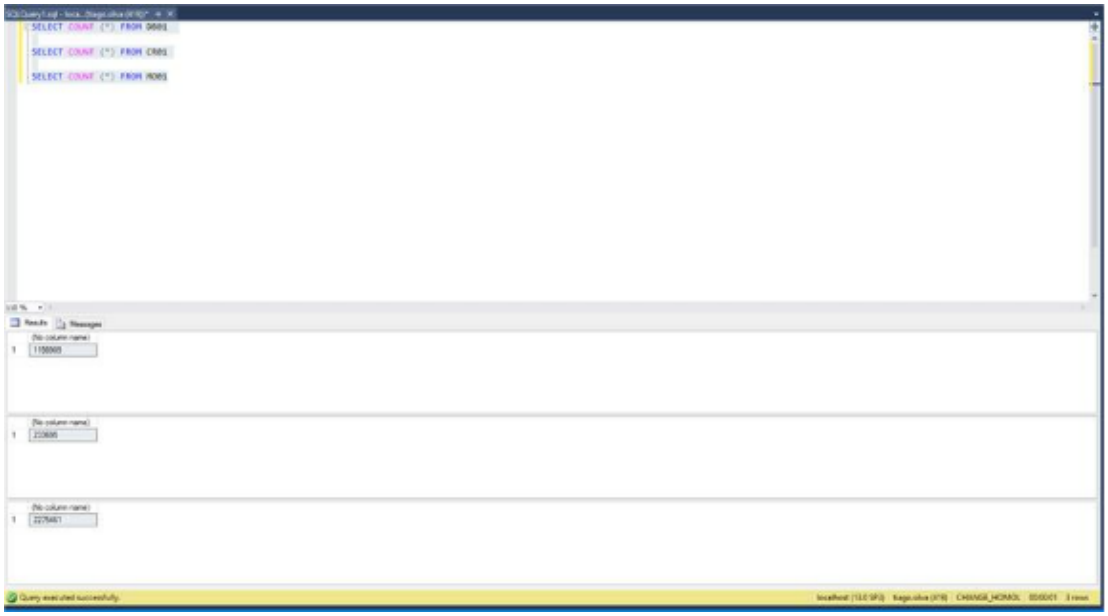

Figura 11 - Etapa 3: Verificação dos dados em ambiente de homologação

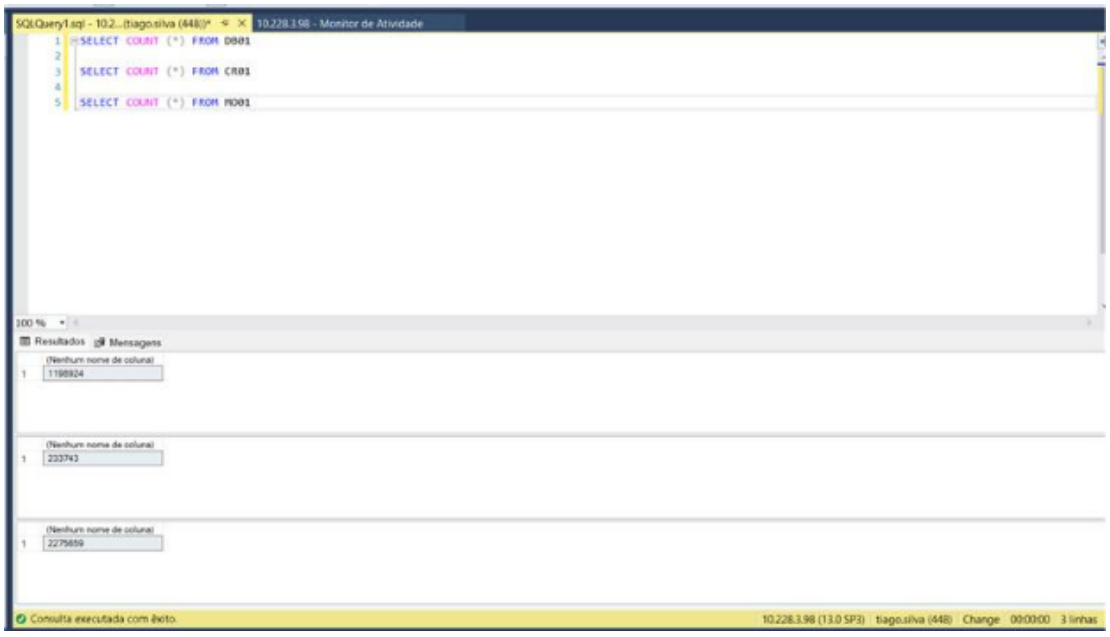

Figura 12 – Etapa 3: Ambiente de Produção para comparação

Após a conferência dos dados, deve-se acessar o sistema, tanto o ambiente de homologação quanto o de produção.

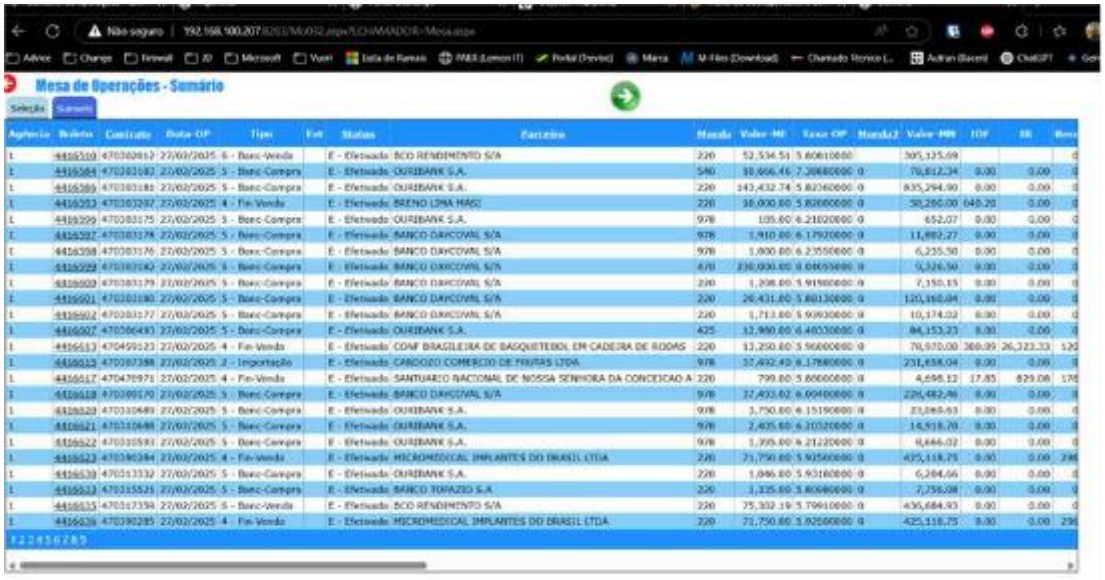

Figura 13 – Etapa 4: Acesso ao Sistema (Homologação)

Figura 14 – Etapa 4: Acesso ao Sistema (Produção)

5. Comunicação e Dúvidas

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

6. 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.

7. 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

Anexos

ANEXO 1 – Fluxo de Backup e Restore