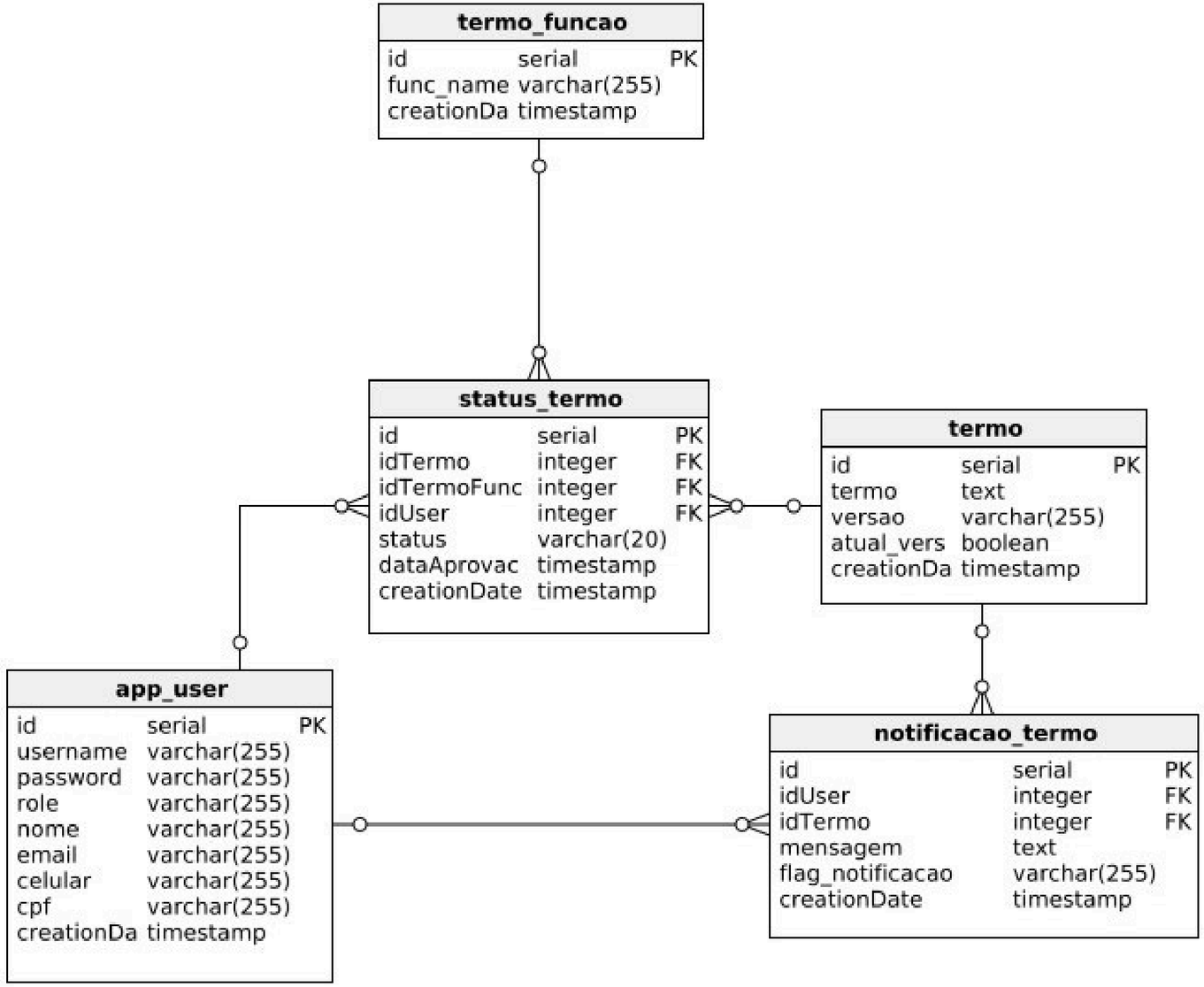
LGPD

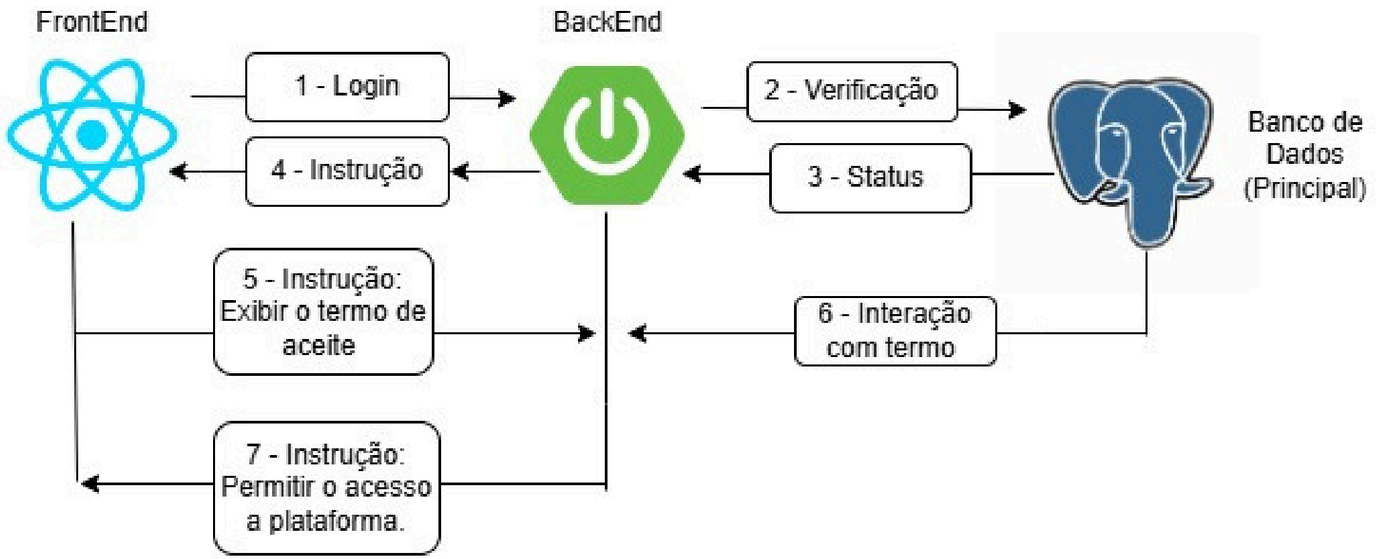
Tópicos

- Termo de Aceite
- Atualização de Dados
- Delete de Usuários
- Notificação de Incidente de Segurança

Termo de Aceite

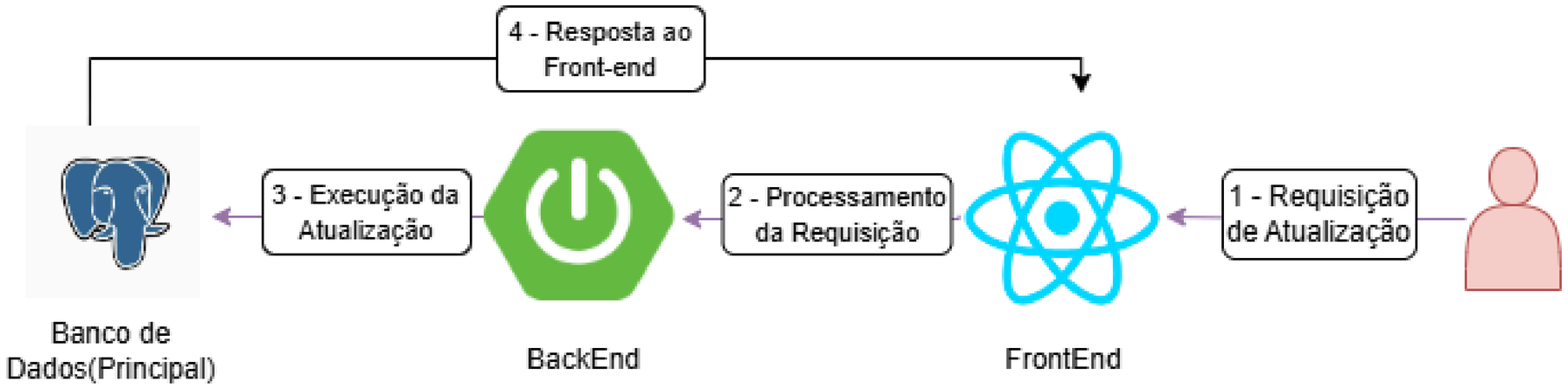


Termo de Aceite



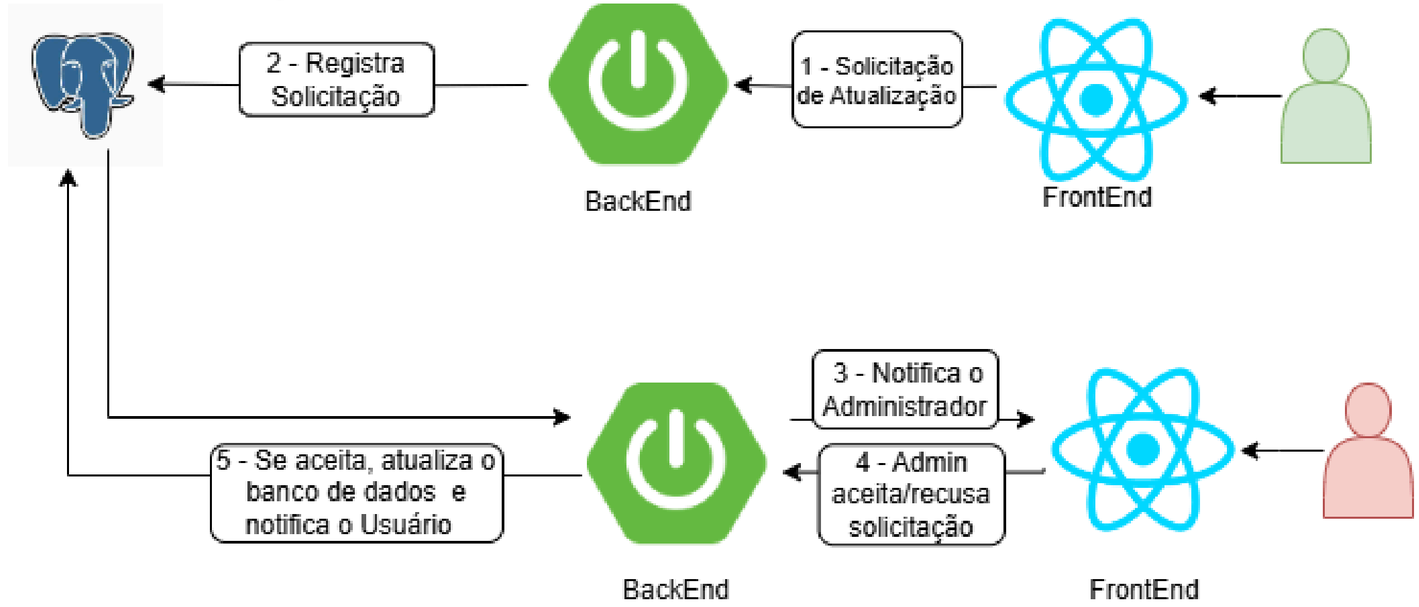
1. O frontend envia uma requisição para o backend.
2. O backend consulta o banco de dados para verificar o status do termo de aceite.
3. O backend determina se é necessário exibir o termo de aceite ou permitir o acesso à plataforma com base no status do termo.
4. O backend envia uma instrução para o frontend.
5. Se necessário, o frontend exibe o termo de aceite.
6. O usuário interage com o termo de aceite, se aplicável.
7. O backend envia uma instrução para permitir ou negar o acesso à plataforma, dependendo da interação do usuário com o termo de aceite.

Atualização de Dados (Usuário Administrador)



1. O usuário envia uma solicitação de atualização de dados através da interface do usuário (front-end).
2. O back-end recebe a solicitação e processa-a, aplicando as regras de negócio necessárias e preparando os dados para atualização.
3. O back-end executa a atualização no banco de dados, que pode envolver a modificação, inserção ou exclusão de registros, conforme necessário.
4. Após a conclusão da atualização, o back-end responde à interface do usuário com uma confirmação ou feedback sobre o resultado da operação. A interface do usuário recebe a resposta do back-end e pode atualizar sua exibição para refletir as mudanças feitas nos dados.

Atualização de Dados (Usuário Comum)



1. O processo começa quando um usuário comum acessa o sistema e solicita a atualização de um dado específico. Essa solicitação é enviada para o front-end do sistema.

2. O back-end registra a solicitação no banco de dados para revisão posterior.

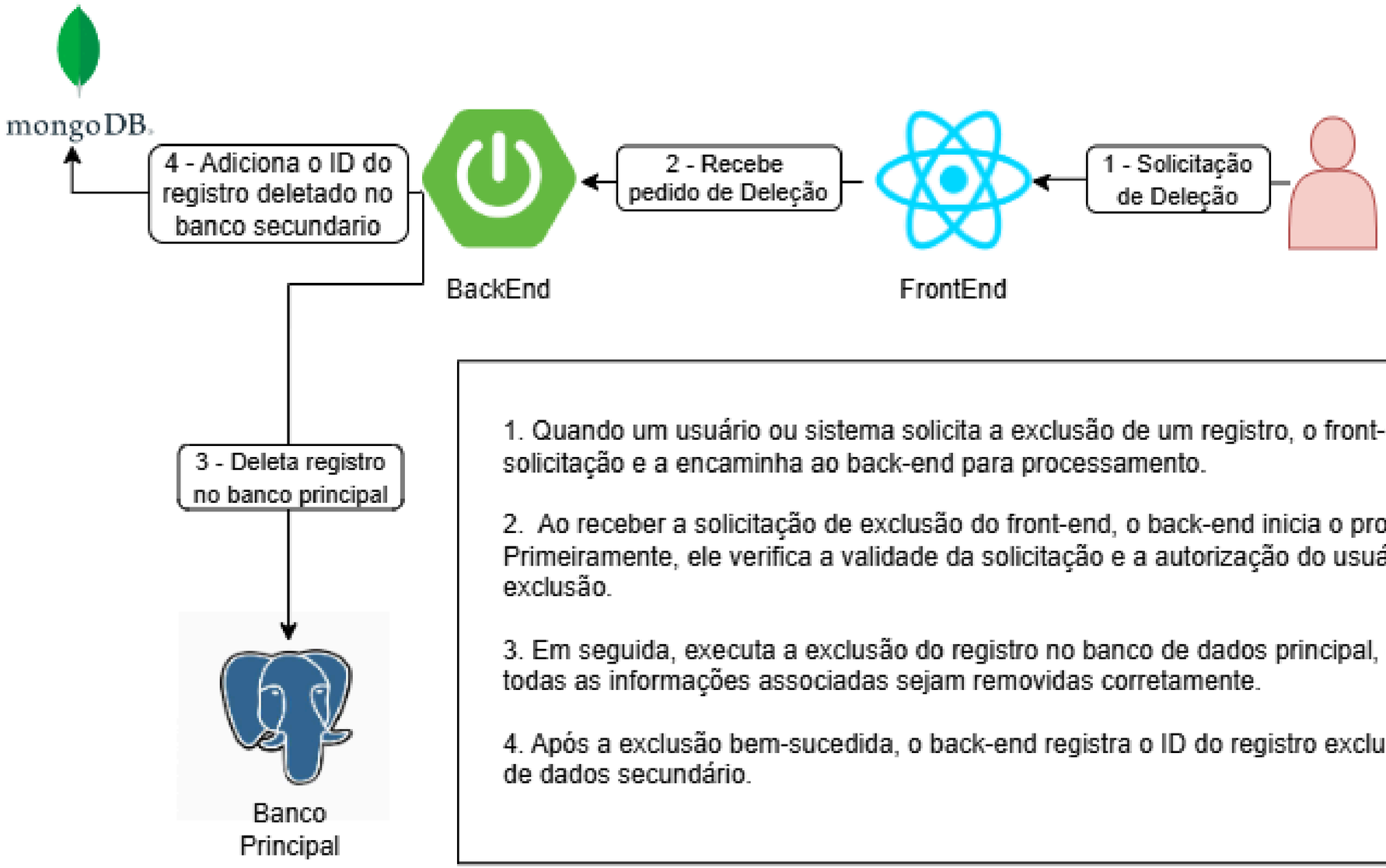
3. Uma vez registrada a solicitação, o back-end notifica o administrador sobre a solicitação pendente. Isso garante que o administrador esteja ciente e possa tomar uma decisão sobre a solicitação.

/

4. O administrador revisa a solicitação e decide se aceita ou recusa. Se a solicitação for aceita, o administrador autoriza a atualização dos dados. Caso contrário, a solicitação é recusada e nenhuma alteração é feita.

5. Se o administrador aceitar a solicitação, o back-end atualiza o banco de dados com os novos dados fornecidos pelo usuário comum. Esses dados atualizados agora estão disponíveis para uso no sistema.

Delete De Usuário



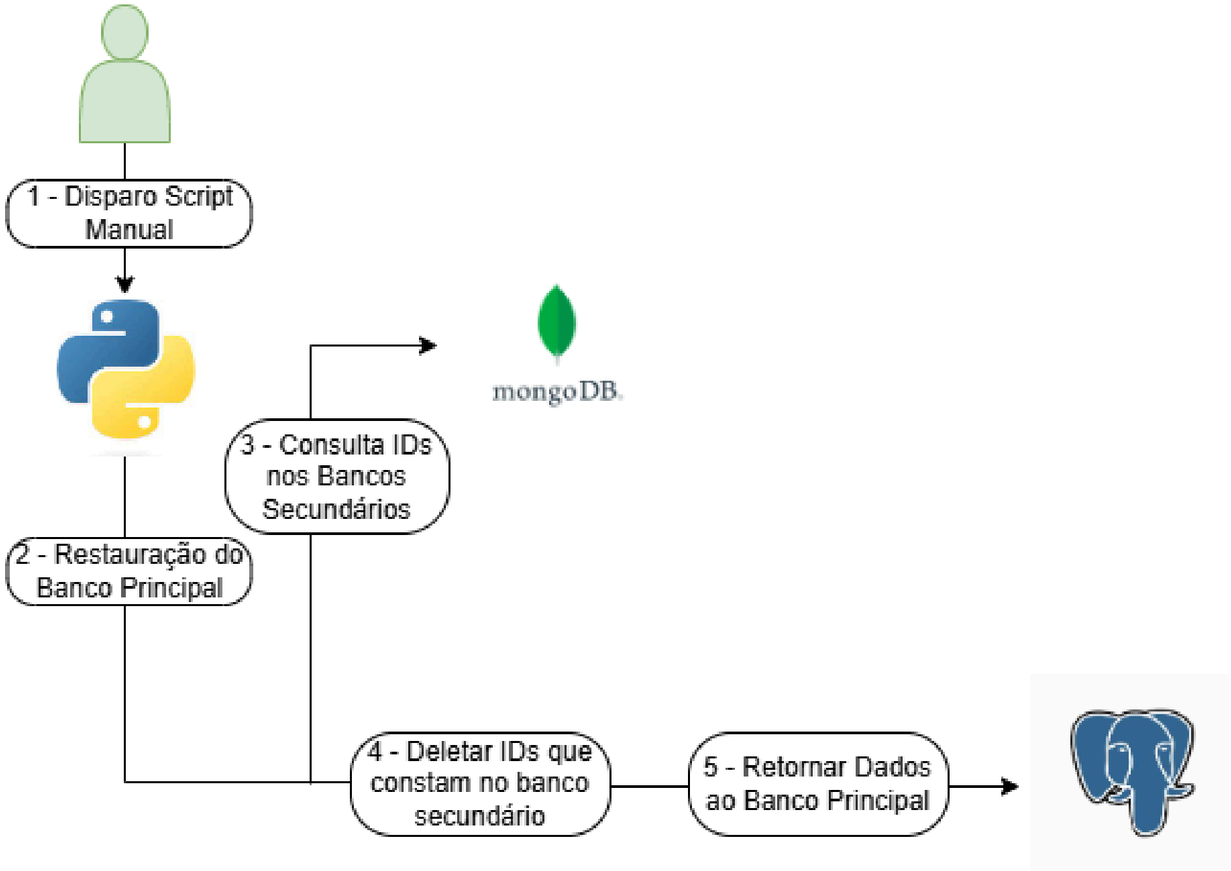
1. Quando um usuário ou sistema solicita a exclusão de um registro, o front-end captura essa solicitação e a encaminha ao back-end para processamento.

2. Ao receber a solicitação de exclusão do front-end, o back-end inicia o processo de exclusão. Primeiramente, ele verifica a validade da solicitação e a autorização do usuário para realizar a exclusão.

3. Em seguida, executa a exclusão do registro no banco de dados principal, garantindo que todas as informações associadas sejam removidas corretamente.

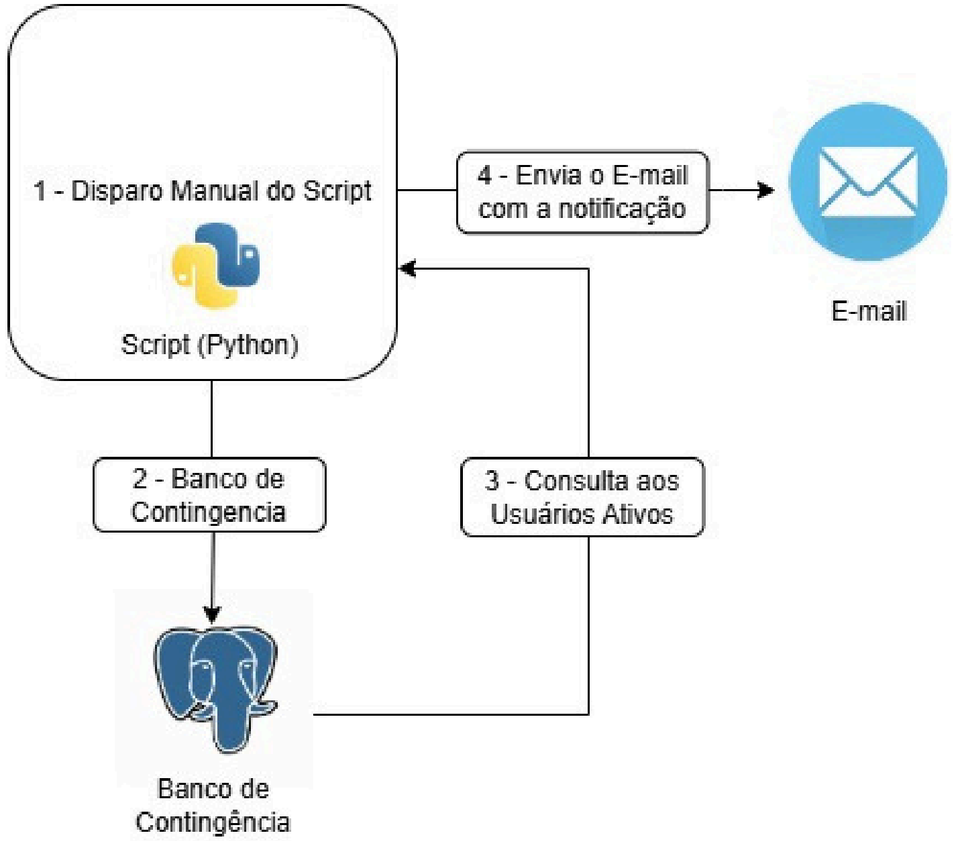
4. Após a exclusão bem-sucedida, o back-end registra o ID do registro excluído em um banco de dados secundário.

Em caso de Restore no Banco (Delete)



1. Disparo do script.
2. O banco de dados principal é restaurado.
3. O script consulta os bancos secundários para obter os IDs que estão na blacklist.
4. Os IDs obtidos que estão na blacklist são deletados dos bancos secundários.
5. Os dados são retornados ao banco principal após a consulta e exclusão dos IDs da blacklist.

Notificação de Incidente de Segurança



1. O operador dispara manualmente o script de resposta ao vazamento de dados.
2. O script cria um backup dos dados comprometidos e estabelece um banco de dados secundário para contingência.
3. O script consulta o banco de dados de contingencia para obter os emails dos usuários afetados.
4. Usando os emails obtidos, o script envia notificações aos usuários afetados sobre o vazamento de dados.

Hi Mailtrap

From: Private Person <fluffyfatec0@gmail.com>
To: <Michealfelipe123@gmail.com>

2024-06-05 00:08, 1.7 KB

Show Headers

HTML | HTML Source | Text | Raw | Spam Analysis | Tech Info

Dear Users,

I hope this message finds you well.

We regret to inform you that our system has recently experienced a security incident. Our database was compromised by a hacker attack, and we are diligently working to understand the full scope of the breach.

We want to assure you that we are taking all necessary steps to mitigate this incident and ensure the safety of your data. Upon identifying the breach, we immediately:

Isolated the affected systems to prevent further damage.
Hired cybersecurity experts to conduct a thorough investigation.
Are collaborating with the appropriate authorities to investigate the origin of the attack.
We are conducting a meticulous analysis to determine which data may have been accessed. At this time, we recommend the following preventive actions for all our users:

Change your passwords immediately. If you use the same password on other services, we suggest changing it there as well.
Be vigilant for any suspicious activity in your accounts and financial statements.
Do not share personal information through unsolicited emails or messages.
We understand the seriousness of this situation and the concern it may cause. The privacy and security of our users are of utmost importance to us, and we are committed to addressing this issue with the highest transparency and efficiency.

We will keep everyone informed about the progress of the investigation and any further actions that may be necessary. We appreciate your patience and understanding as we work to resolve this matter.

If you have any questions or need additional assistance, please contact our support team at fluffyfatec0@gmail.com.

Sincerely,

Fluffy