globo.com

Gerenciamento de Senhas

Agenda

- Motivação
- Métodos utilizados para armazenamento de senhas
- Principais *softwares* utilizados
- Compartilhando uma senha
- GSenha

Motivação

- Dificuldade em gerar uma senha complexa
  - Alfanumérica, caracteres especiais, mínimo de lógica possível

senha

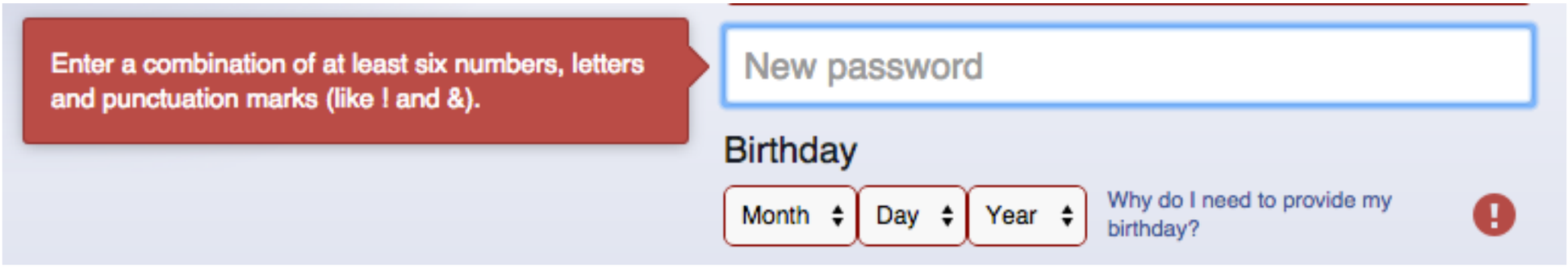
confirmar a senha

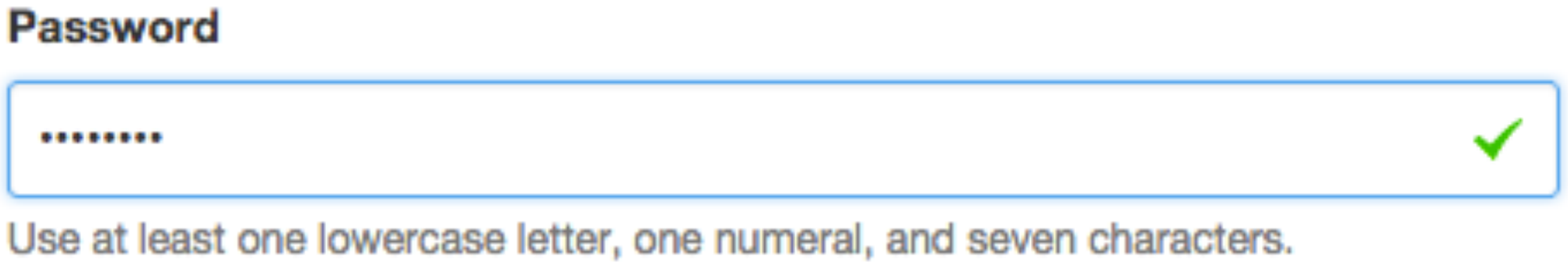
Escolha uma senha de 8 a 15 caracteres.
Recomendamos combinar letras minúsculas com maiúsculas e números.
Porém não utilize caracteres especiais como *, $, %, #, etc.
Veja algumas dicas.

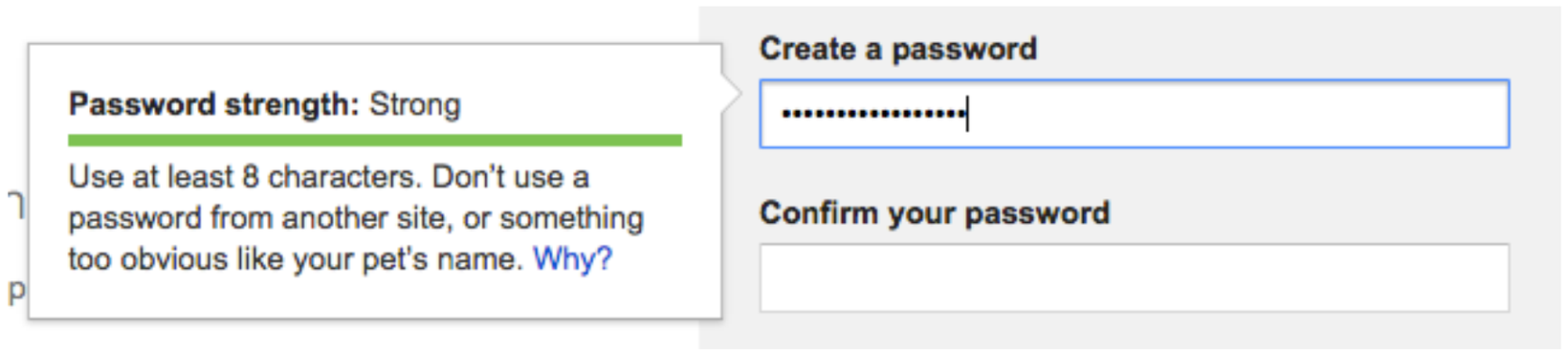
DICAS DE SEGURANÇA

- Evite senhas com nível de segurança moderado;
- Cuidado com senhas fáceis de outras pessoas adivinharem. Exemplo:
  - Seu nome ou de alguém próximo;
  - Sequências como "1234", "abcd", etc;
  - Palavras óbvias: Jesus, amor, etc;
  - Datas comemorativas: aniversário, casamento, etc;
- Troque sua senha com frequência;
- Combine letras minúsculas com maiúsculas e números;
- Evite usar a mesma senha em vários lugares.
- Nunca esqueça sua conta logada em computadores públicos;
- Relacione sua senha com alguma frase fácil de lembrar.

voltar ao cadastro


Enter a combination of at least six numbers, letters and punctuation marks (like ! and &).
New password
Birthday
Month
Day
Year
Why do I need to provide my birthday?


Password
Use at least one lowercase letter, one numeral, and seven characters.


Password strength: Strong
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?
Create a password
Confirm your password

"Sorry, your password must contain a capital letter, two numbers, a symbol, an inspiring message, a spell, a gang sign, a hieroglyph and the blood of a virgin"

Motivação

- Grande número de senhas
  - Diversos sistemas e serviços
  - Memorização
- Sistemas críticos
  - Senhas ainda maiores
  - Geralmente geradas aleatoriamente

Como armazenar tanta senha?

- Algumas soluções “práticas" utilizadas

Primeira solução

- Para que tanta senha diferente?
- Vou utilizar apenas uma para todos os serviços, assim só preciso lembrar dessa

Primeira solução

- NÃO!
- Alguma base de dados de algum serviço que você utiliza irá vazar
- E a sua senha estará armazenada de forma errada <plaintext>
- Tudo estará perdido

Segunda solução

- Vou criar senhas simples e fáceis de memorizar
- Data de aniversário, nome do animal de estimação, nome do irmão, nome da mãe, da avó…

Segunda solução

- NÃO!
- Uma simples engenharia social (conversa no bar) revela todas essas informações

Terceira solução

- Gerar senhas complexas e difíceis de serem memorizadas
- Guardar tudo em um arquivo *senhas.txt* ou em uma planilha

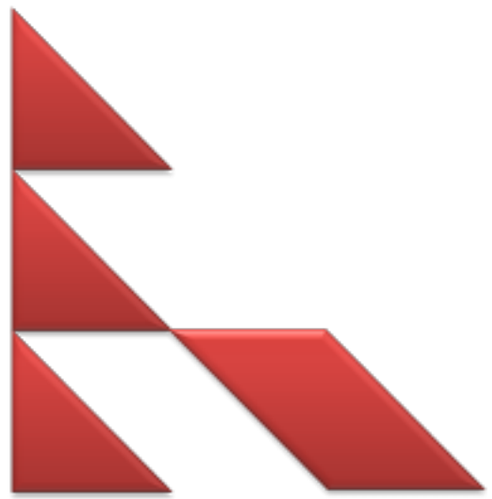
senhas.txt

Gmail: 1i32ndH#uhd1d
Facebook: fldh23d#@UDH*!@#
Github: lHqeolF<MxNC7*!
Internet banking: 123456
Cartão: 987654
Email corporativo: P;lfH#9^@!,>shdEOMchaR123

Quarta solução

- Utilizar um *software* que faz o gerenciamento de senhas
  - A base de dados é encriptada com uma chave mestra fornecida pelo usuário
- É necessário guardar apenas uma senha complexa (a chave mestra) e quando necessário consultar a base de dados

Principais *softwares* utilizados

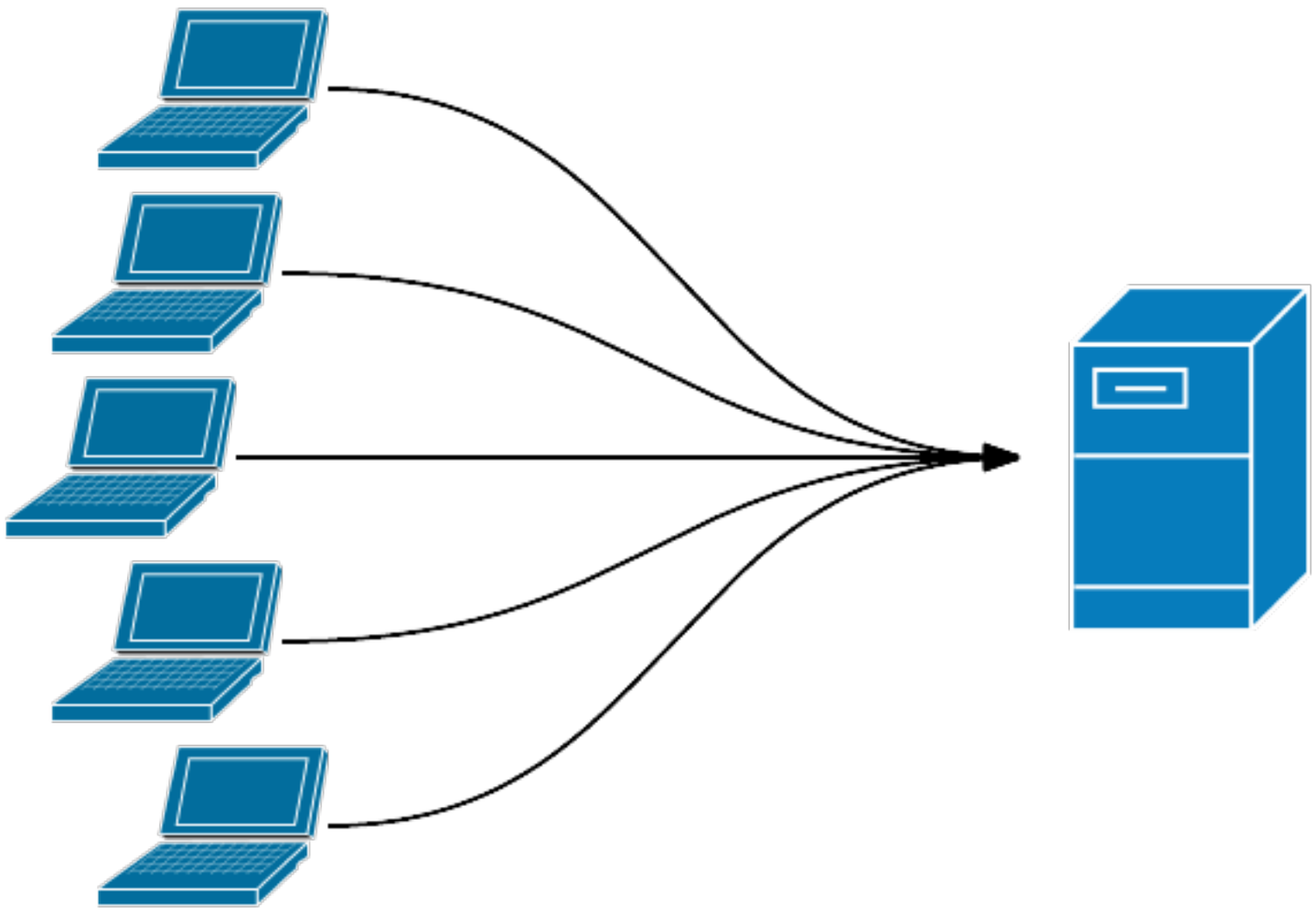


Como compartilhar uma senha?

- Senha de *root,* senha de administradores, senhas de serviços que não é possível ter um *login* para cada um, senhas de equipamentos, senhas de banco de dados, e etc…

Como compartilhar uma senha?

- Mesmo arquivo, mesma chave mestra



Como compartilhar uma senha?

- Inconsistência
- Sempre que alterado todos tem que copiar novamente para a máquina local
- Editar o arquivo compartilhado pensando que era o pessoal
- Mesma chave mestra

GSenha

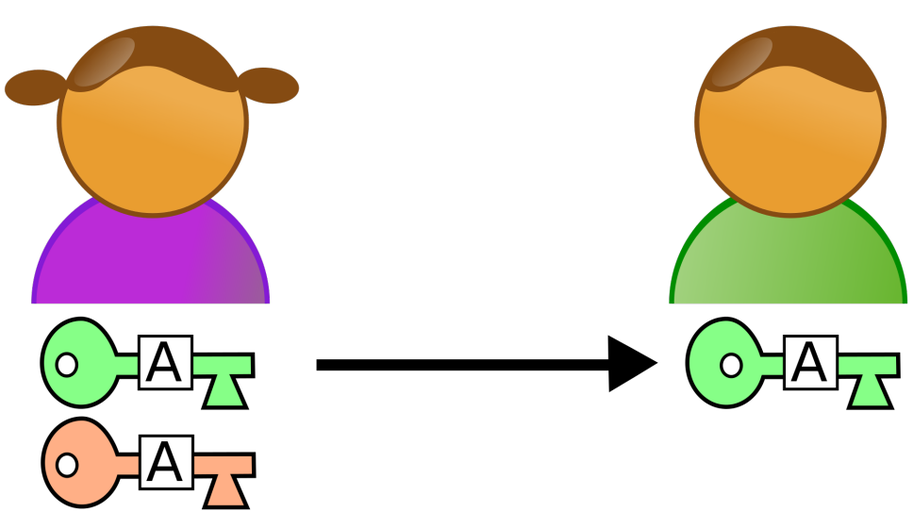
- Sistema simples
- Atende as necessidades
- Resistente a vazamento de dados

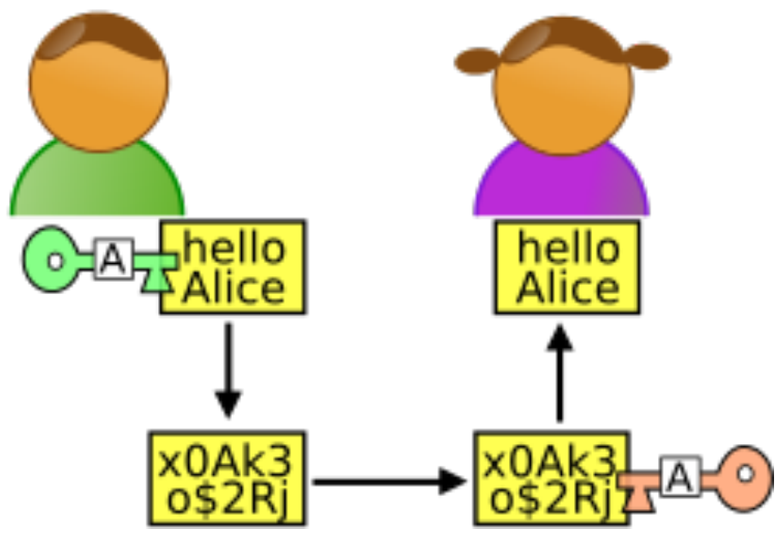
GSenha - estrutura

- O GSenha é feito de um conjunto de uma API REST com um *front-end* que consome essa API
  - A API pode ser consumida diretamente, e qualquer um pode fazer um *front-end* da maneira que quiser
- Desenvolvimento feito em python, utilizando o *microframework* Flask
- O tráfego entre o usuário, os servidores e banco de dados deve ser feitos via HTTPS

GSenha - criptografia

- Criptografia assimétrica





- Chave RSA com 4096 bits

GSenha

- Autenticação e permissionamento feito via LDAP
- O usuário se "auto-adiciona" no sistema
  - Ao se adicionar informa a sua chave pública, que é armazenada no banco de dados
  - A chave privada nunca é armazenada no banco de dados

GSenha - funcionalidades

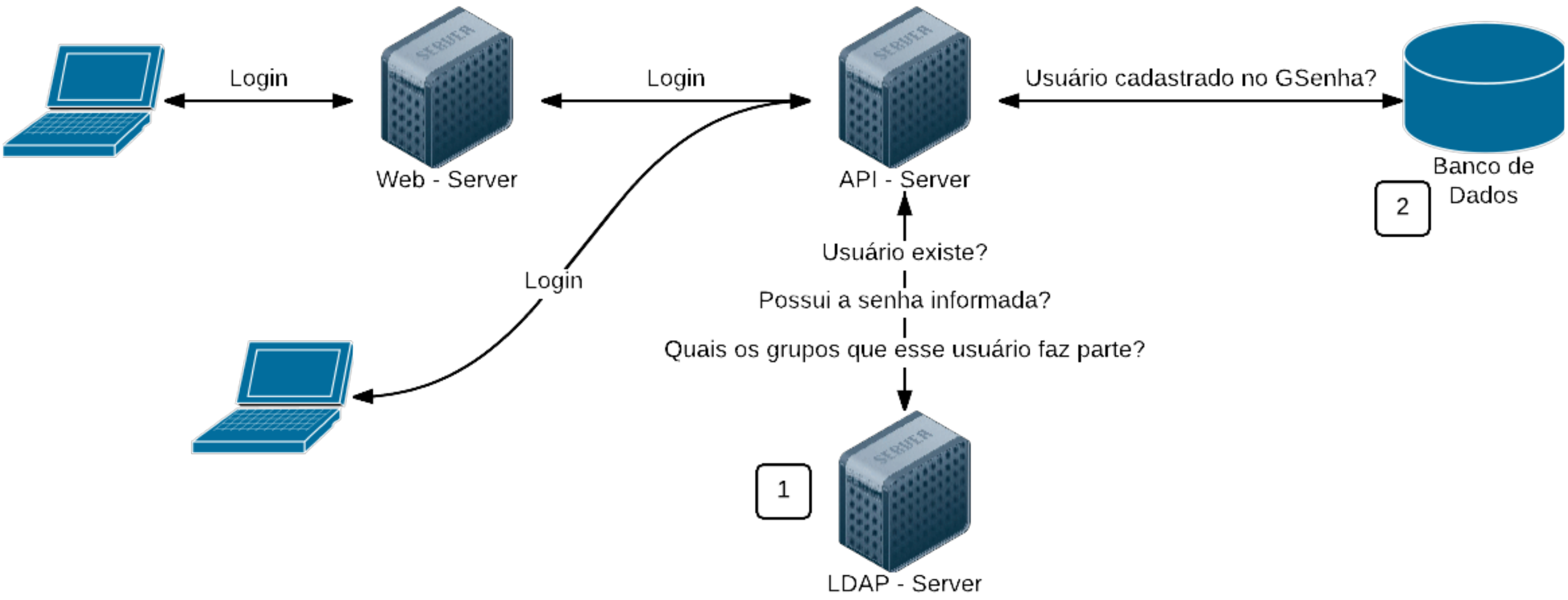
- Adição de senha pessoal
- Adição de senha compartilhada
- Adição de senha para um outro usuário (quem adicionou não irá conseguir visualizar essa senha)
- Adição de senha compartilhada para um outro grupo (quem adicionou não irá conseguir visualizar essa senha)

GSenha

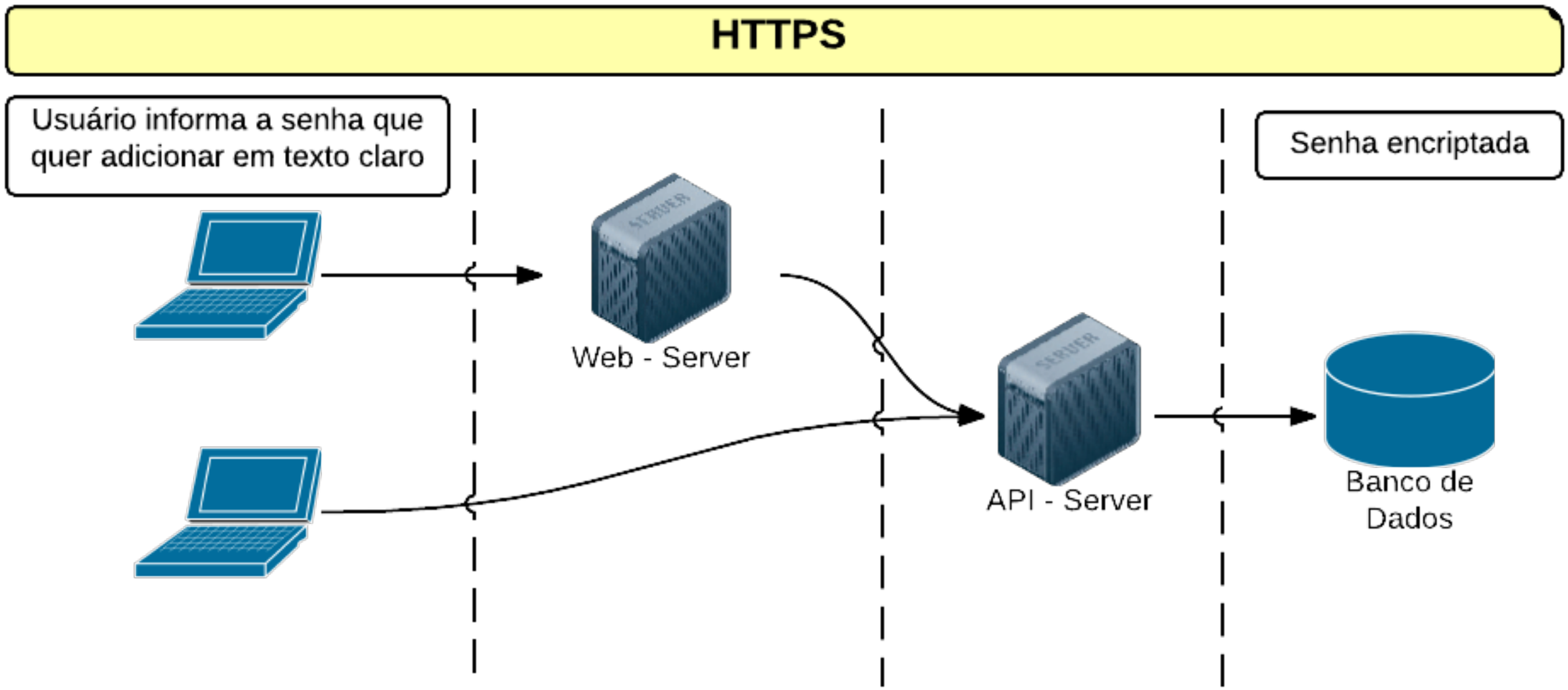
- Uma pasta pessoal por usuário aonde só ele tem poder de visualização
- Pastas de grupo aonde todos os membros tem poder de visualização

GSenha - Login

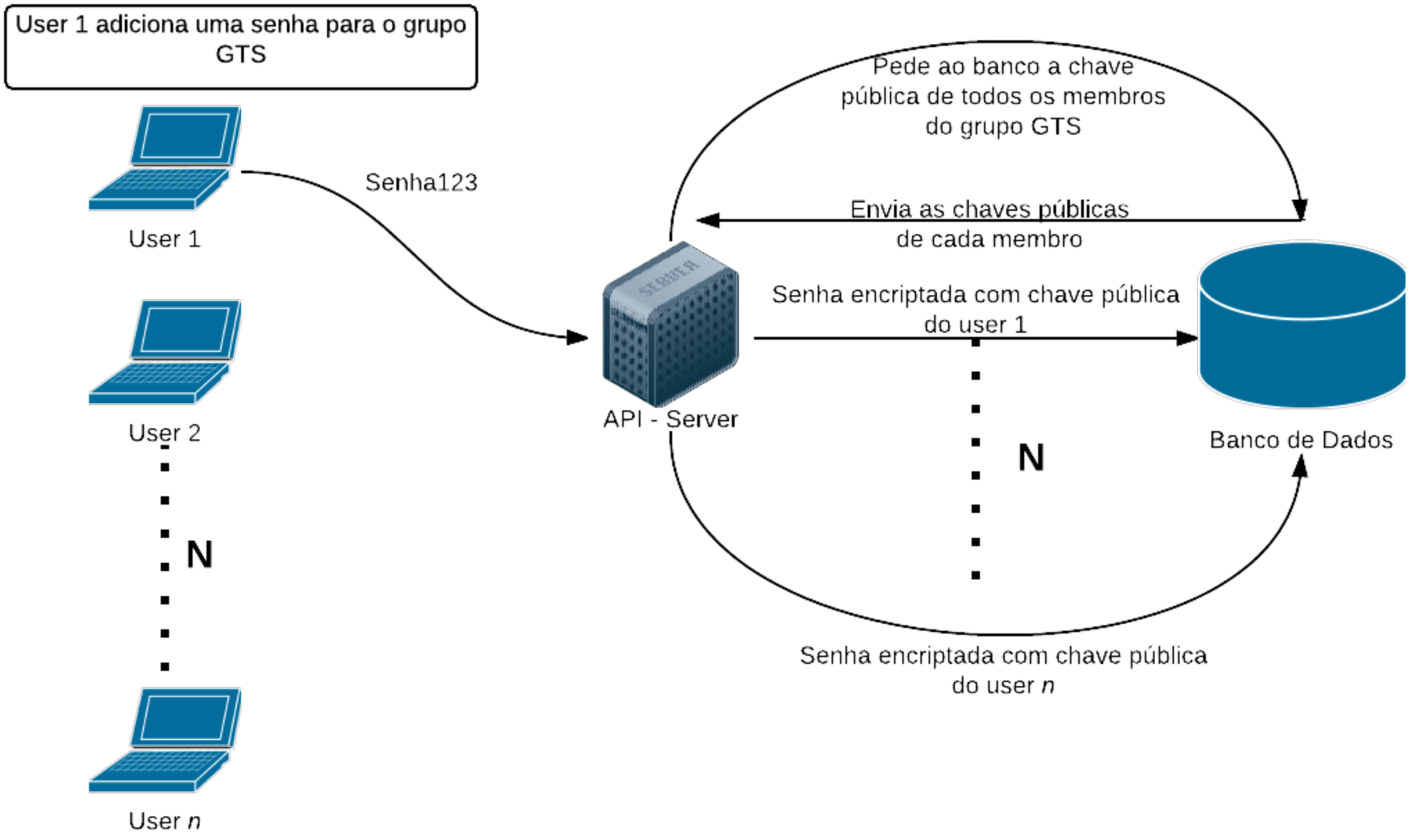
- Exemplo de Login



GSenha - adição de senha pessoal



GSenha - adição de senha compartilhada



GSenha - problema gerado pelas senhas compartilhadas

- Seguinte cenário: existem quatro (4) usuários em um determinado grupo, e eles adicionam senhas compartilhadas. Todos conseguem visualizar sem problemas, as senhas serão adicionadas com suas respectivas chaves públicas.
- Entra um novo usuário nesse mesmo grupo, como que ele irá visualizar as senhas se ele não tinha uma chave pública cadastrada?

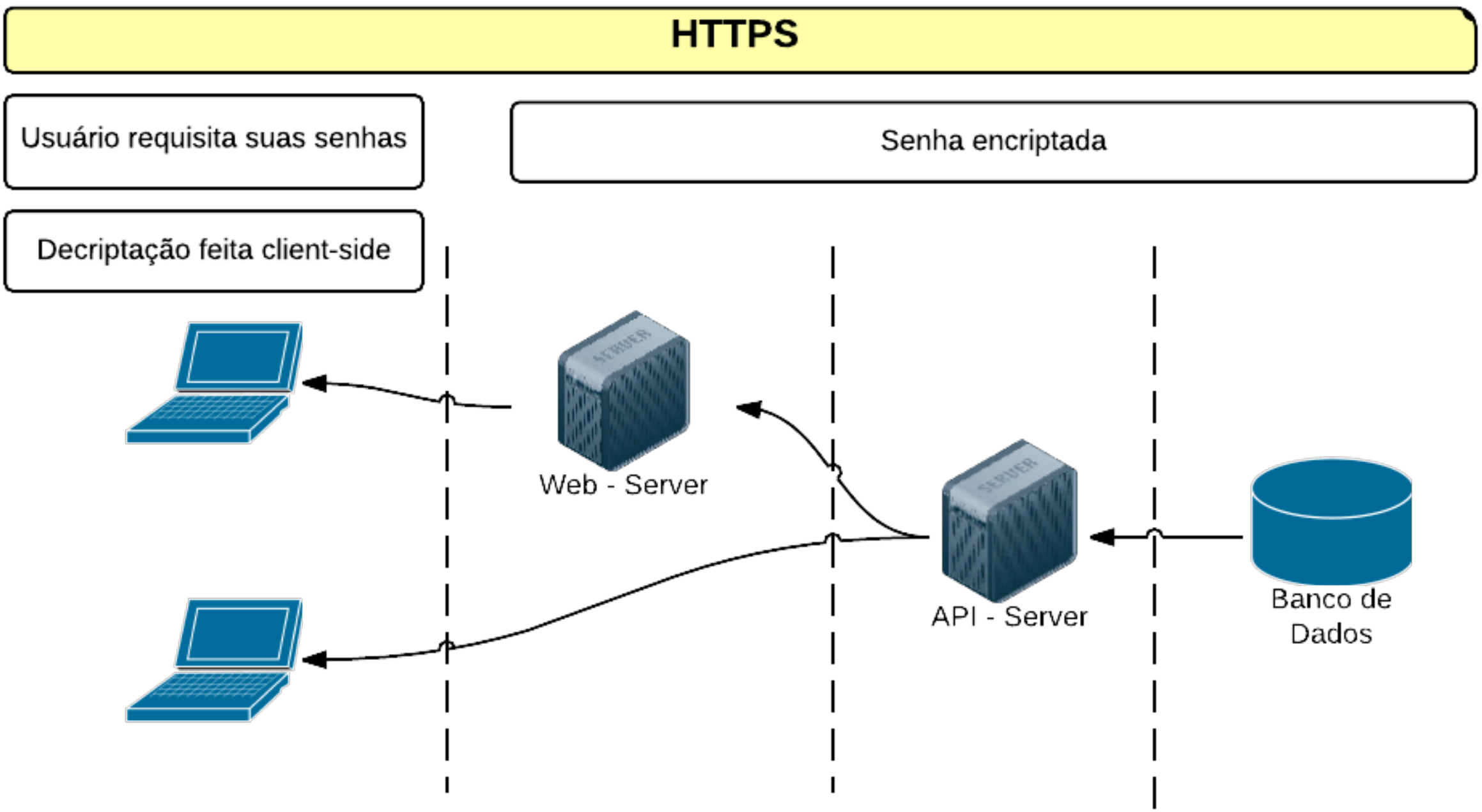
GSenha - solução

- É necessário "desbloquear" esse novo usuário
- Alguém que tenha acesso as senhas deverá fazer esse processo
- Informar o *username* do usuário que quer ser desbloqueado e a chave privada de quem está fazendo o desbloqueio

GSenha - consulta de senhas

- Ao fazer o *login* no sistema, uma requisição é feita para a API que responde com todas as senhas que aquele usuário tem permissão de visualizar
- As senhas são enviadas todas encriptadas
- O processo de decriptação é feito *client-side*

GSenha - consulta de senhas



GSenha - consulta de senhas

- $ curl -vvv -H "Content-Type: application/json" -d '{"user":"usuário","password":"senha"}' [GSENHA_API]/get/passwords

GSenha - consulta de senhas

{

"Personal Passwords": {

"/Personal/Felipe": [

{

"ID": 1,

"description": “senha de root",

"login": "root",

"name": "Senha Teste",

"password": “LOT+Ctu8UbTIfFWwzMX/kdBcja2…”

“url”:”globo.com”

GSenha

GSenha

GSenha

Username

Password

Private Key

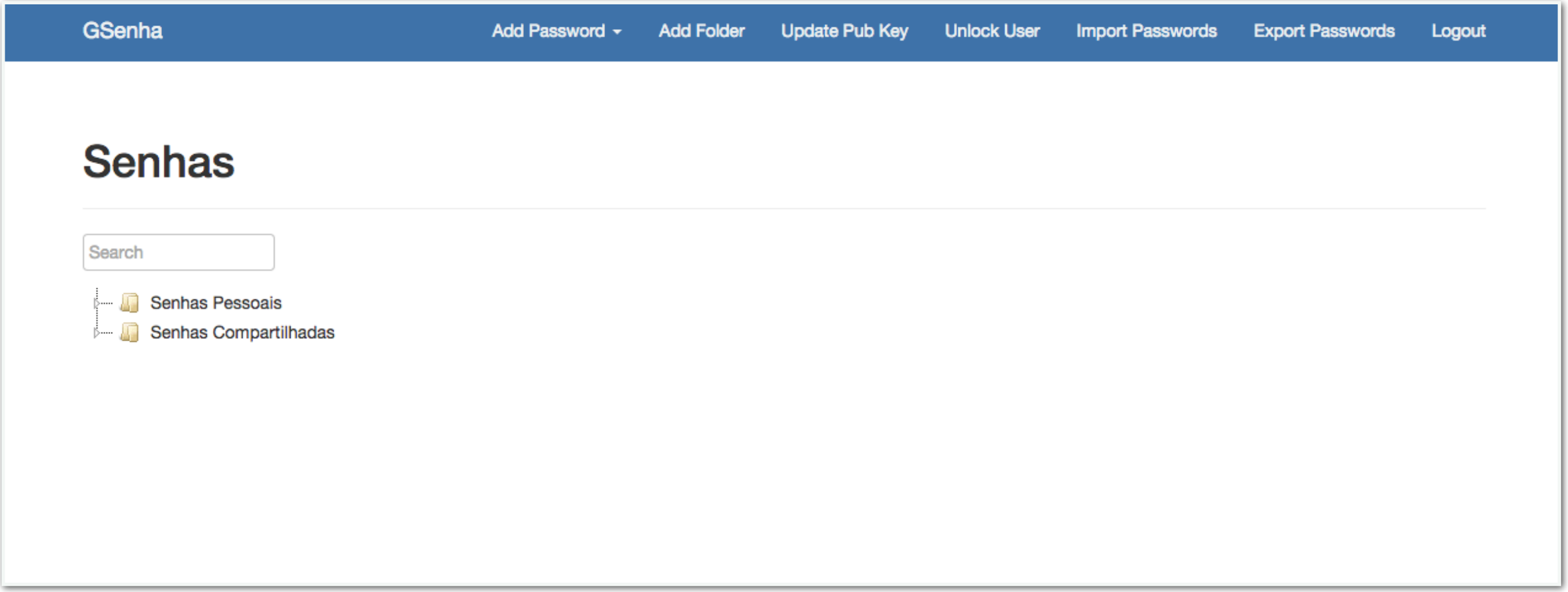
Copie e cole a sua chave privada ou escolha o arquivo a seguir.

Privte Key File

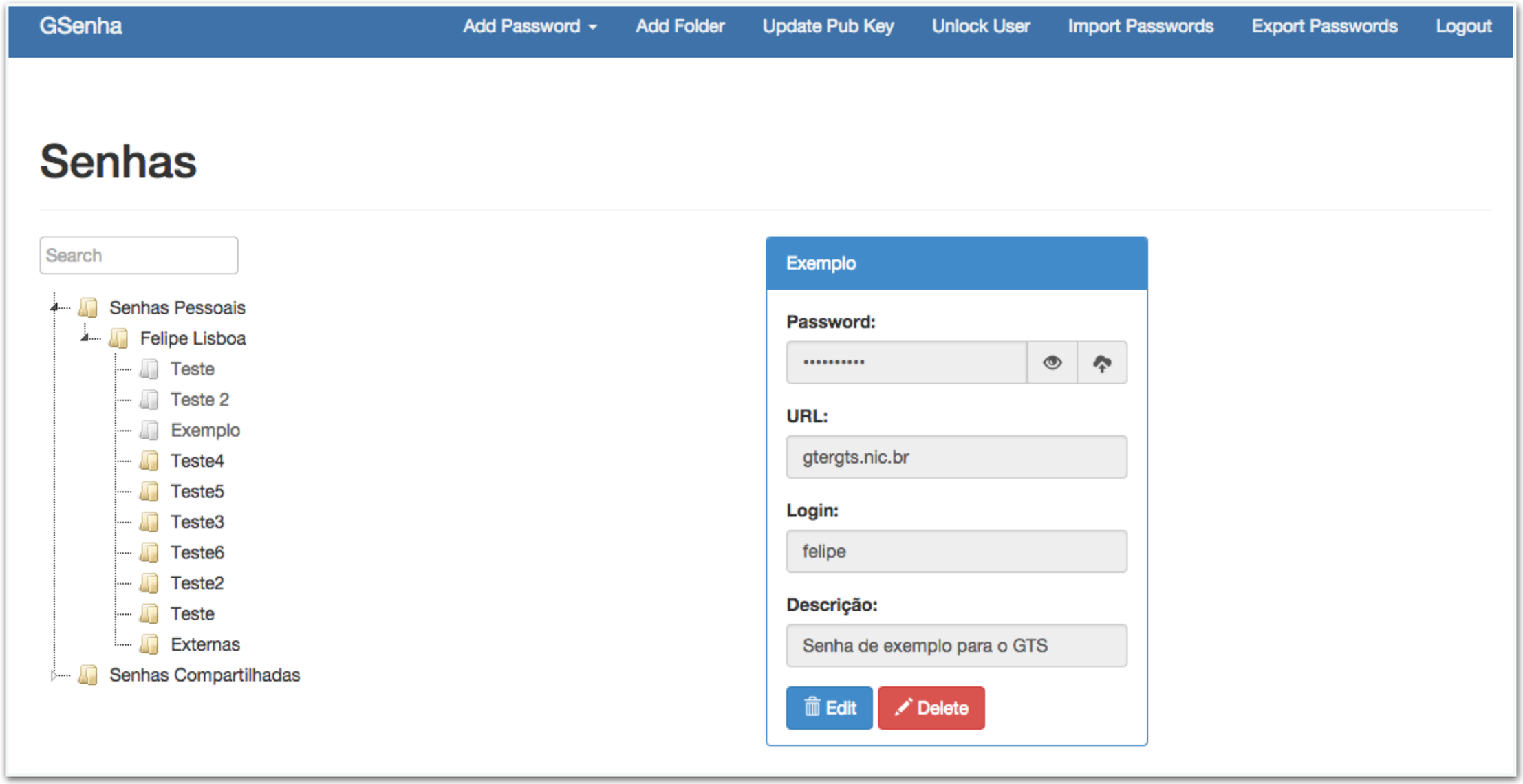
Choose File No file chosen

Submit

GSenha


GSenha
Add Password
Add Folder
Update Pub Key
Unlock User
Import Passwords
Export Passwords
Logout
Senhas
Search
Senhas Pessoais
Senhas Compartilhadas

GSenha


GSenha
Add Password
Add Folder
Update Pub Key
Unlock User
Import Passwords
Export Passwords
Logout
Senhas
Search
Senhas Pessoais
Felipe Lisboa
Teste
Teste 2
Exemplo
Teste4
Teste5
Teste3
Teste6
Teste2
Teste
Externas
Senhas Compartilhadas
Exemplo
Password:
URL:
gtergts.nic.br
Login:
felipe
Descrição:
Senha de exemplo para o GTS
Edit
Delete

GSenha - visualização das senhas com fator duplo

- Senha de autenticação (fator que o usuário sabe)
- Chave privada para decriptação (fator que o usuário possui)

GSenha - modelagem de ameaças

- O GSenha não tem mecanismos de proteção contra atacantes que tenham acesso ao Banco de Dados
- Um indivíduo malicioso com acesso ao BD poderá apagar, alterar e expor os dados ali armazenados
- As senhas **não** serão comprometidas, todas estarão criptografadas, e a chave privada **não** está armazenada no BD

GSenha - modelagem de ameaças

- O GSenha não tem mecanismos de proteção contra atacantes que tenham acesso aos servidores aonde o sistema está rodando
  - Um indivíduo malicioso com acesso aos servidores poderá fazer um *dump* da memória e visualizar senhas em texto claro - quando um usuário acaba de mandar uma requisição de adição de senha

GSenha - modelagem de ameaças

- Um usuário que tenha acesso ao sistema, e que faça parte de algum grupo pode simplesmente copiar manualmente todas as senhas

GSenha - fallback

- O sistema **NÃO** possui nenhum sistema de *fallback*
- Se um usuário perder a sua chave privada não conseguirá visualizar suas senhas pessoais novamente
- Em senhas compartilhadas, desde que pelo menos um usuário pertencente ao grupo tenha a chave privada é possível recuperá-las

Obrigado!

felipe.lisboa@corp.globo.com

Em breve em:
http://opensource.globo.com/