

Especificação do Painel VPN

Uma grande parte das organizações utilizam VPN para aumentar a segurança quando o assunto é Home Office, mas infelizmente enviam o mesmo certificado para todos os usuários, e isso é um problema. Em caso de revogação de acesso por certificado temos um grande problema pois ao revogar um certificado único paramos toda a organização. Em contrapartida, para gerar um certificado para cada funcionário, encontramos um exaustivo trabalho de gestão de certificados.

O objetivo deste sistema que está sendo proposto é delegar aos funcionários a obtenção e gestão dos certificados de acesso, para isso o funcionário poderá entrar em um painel e obter um novo certificado ou revogar um certificado existente.

1.1 Persona envolvida

O sistema possui apenas duas personas envolvidas no processo, que são os funcionários que estão em home office bem como o administrador que faz a gestão de cadastro de funcionários. Então o administrador pode:

- I. Cadastrar novos funcionários;
- II. Eleger novos administradores;
- III. Revogar administradores;
- IV. Revogar acesso de funcionários;
- V. Ativar acesso de funcionários;
- VI. Remover o cadastro de um funcionário;

Além destas funções, o administrador é um funcionário, então pode o que todo funcionário pode fazer, que é:

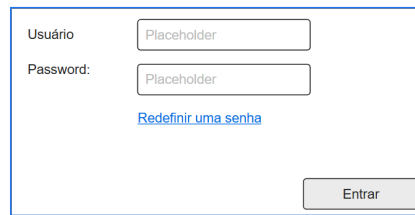
- VII. Criar um novo certificado para acesso pela VPN;
- VIII. Remover um certificado de acesso;

1.2 Layout geral do sistema

O sistema será formado por duas áreas, uma primeira área pública contendo apenas uma interface de **Login** e **Redefinição de senha**. A segunda área terá as interfaces com as funcionalidades requeridas.

1.2.1 Interface de Login

Com certeza uma das telas mais complexas devido a sua exposição, então devemos estar atento às operações de injeção, deverá ser uma tela limpa com poucos elementos, com destaque para o logo da empresa.



Form de login do painel VPN. Possui campos para 'Usuário' e 'Password', ambos com placeholders. Abaixo do campo de senha há um link 'Redefinir uma senha'. Um botão 'Entrar' está na parte inferior direita.

Na interface acima temos que garantir que o usuário informe todos os campos, então:

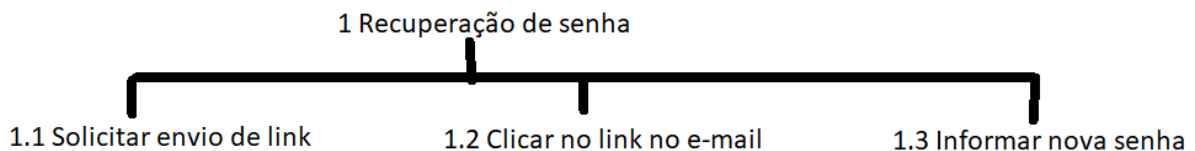
- Caso não informe o username devemos exibir a seguinte mensagem: **Informe o username para realizar o processo de entrada;**
- Caso não informe o password devemos exibir a seguinte mensagem: **Informe o password do usuário para realizar o processo de entrada;**

Caso informe o username e password, estando errada a relação entre eles devemos exibir a seguinte mensagem: **Usuário ou senha estão incorretos**. Esta também será a mensagem se o usuário não existir. Se o usuário fizer **10 tentativas** erradas então deve-se revogar o acesso do usuário no painel. Se foi revogado o acesso e o usuário tentar logar novamente, deve aparecer a mensagem: **Entre em contato com o administrador da rede**.

O campo de senha deve ter como caracteres apenas asteriscos, enquanto um username deve ter no mínimo 3 caracteres e no máximo 30 caracteres.

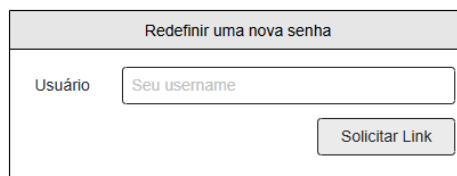
1.2.2 Interface de Recuperação de senha

Devemos dar a opção de recuperação de senha, então o funcionário devidamente cadastrado poderá solicitar por e-mail um link e é através do link que o funcionário entrará na opção de redefinição de senha. Segue HTA com a sequência de atividades/eventos.



1.2.2.1 Solicitação de Link

Não se manda um username ou password por e-mail, isso é errado. O que fazemos é gerar um link único que só pode ser clicado apenas 1 vez, que leva para uma interface para que o usuário crie uma nova senha. Então em 1.1 (HTA acima) temos a seguinte interface.



Form de solicitação de link para redefinição de senha. O título é 'Redefinir uma nova senha'. Possui um campo 'Usuário' com o placeholder 'Seu username' e um botão 'Solicitar Link'.

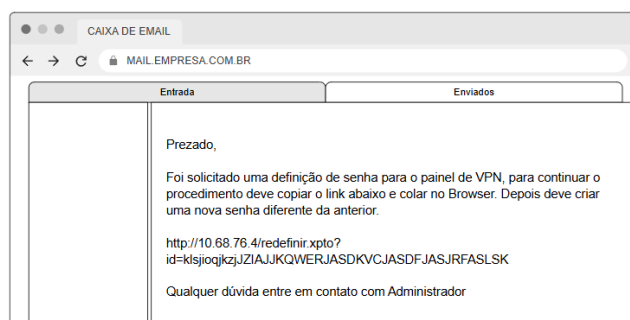
Temos um problema de segurança, nós nunca podemos deixar claro se o usuário existe ou não, é um ponto em que muitos sistemas falham. Vamos assumir um modo muito restritivo afinal se trata de um painel de acesso às configurações de infraestrutura, acertando ou errando o username devemos informar: **“Um e-mail com um link foi enviado para sua caixa de entrada”**.

Como já dito o campo username deve ter no mínimo 3 caracteres e no máximo 30 caracteres. Caso não informe o username devemos exibir a seguinte mensagem: **Informe o username para realizar o processo de entrada;**

A equipe de TI pode utilizar o próprio Postfix instalado no servidor para envio do e-mail e o e-mail sempre será o que está cadastrado no banco de dados para o username informado. Lembre-se que o link gerado deve ser único e também de clique único.

1.2.2.2 Nova senha

Quando é solicitado um link então deve-se enviar o link único para o e-mail do funcionário, então o funcionário clica no link (tópico 1.2 do HTA acima). Conforme figura abaixo (**trata-se de uma interface externa e não é implementada no nosso sistema**).



Será redirecionado para o site da empresa, especificamente para a interface de **Nova Senha** que solicitará uma nova senha e uma confirmação.

| Redefinir uma nova senha | |
|--|---|
| Senha | <input type="password" value="password"/> |
| Confirmação | <input type="password" value="password"/> |
| <p>Deve ter no mínimo 8 caracteres; No mínimo 1 caractere de A-Z; No mínimo 1 dígito de 0-9; um carácter especial como !@#\$%&*-_+=.</p> | |
| <input type="button" value="Confirmar"/> | |

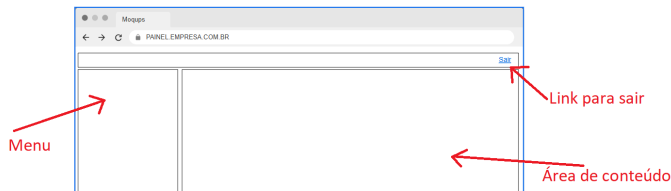
Para prosseguir, o que foi informado nos dois campos devem corresponder, e o usuário errar neste ponto então deve-se dizer: **“A senha informada não corresponde com a confirmação de senha”**, além disso a senha deverá ter (regras):

- no mínimo 8 caracteres;
- tendo no mínimo 1 caractere de A-Z;
- 1 dígito de 0-9;
- um carácter especial como !@#\$%&*-_+=.

Estas regras devem estar bem claras nesta interface. Se estiver tudo certo, então informe para o usuário: **Sucesso, agora você pode realizar a autenticação.** Aproveite e já o redirecione para a interface de **Login**.

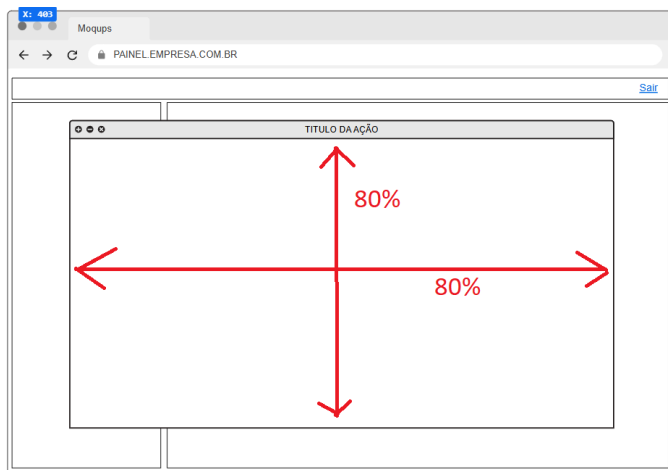
1.2.3 Arcabouço das interfaces após autenticação

A navegação será muito simples, vamos ter as principais ações no menu de opções e acessíveis por lá. Já para as ações menores, dentro da interface, usaremos popup tendo a dimensão de 80% da dimensão do browser.



Veja que no layout principal do sistema temos 3 áreas:

- Área de opções do menu;
- Área de opções de usuário, somente com um link Sair;
- Área de conteúdo;



O popup deve ter um título e deve ocupar 80% da interface, tanto na horizontal quanto na vertical.

As opções de menu devem refletir as personas que o usuário representa na organização, e portanto o usuário Administrador deve ter além de suas opções as opções de um funcionário comum.

Sobre as tabelas, toda coluna deverá ter dois símbolos, um de maior e outro menor. Não será colocado nas tabelas neste texto pois a partir deste ponto assume-se que tem.

| | Nome ▲ ▼ |
|--------------------------|------------------------|
| <input type="checkbox"/> | Amadeu Osório da Silva |

Você deverá ordenar de forma crescente ou decrescente de acordo com o ícone que o usuário pressionou.

Já sobre filtros, toda tela que tem uma tabela deverá ter um campo de busca, sem nenhum botão, o usuário digita algo e pressiona “enter”. Esse filtro deve refletir nas tabelas. Deve estar no canto superior direito.



1.2.4 Layout da área de administração

Conforme já descrito, o administrador pode cadastrar outros funcionários, os links para estas telas só devem aparecer se a pessoa autenticada é um administrador, e lembre-se, se

um funcionário não administrador tentar acessar uma interface de administrador ele não conseguirá o carregamento da interface.

1.2.4.1 Lista de Funcionários e Administradores

Conforme dito, um funcionário pode ser um administrador e os administradores podem elevar o privilégio de funcionários para administração¹. Então devemos exibir uma listagem e nesta listagem ter o botão que adiciona um novo funcionário (requisito I do administrador), este botão deve ficar acima da listagem .

| Editar | | Novo |
|-------------------------------------|-----------------------------|---------------|
| | Nome | Função |
| <input type="checkbox"/> | Antônio Carlos Manoel | Administrador |
| <input checked="" type="checkbox"/> | Amadeu Osório da Silva | Funcionário |
| <input checked="" type="checkbox"/> | Maria Claudia do Nascimento | Funcionário |

Nesta interface deve-se poder filtrar os elementos por nome e para ser realizado o filtro deve-se pressionar Enter.

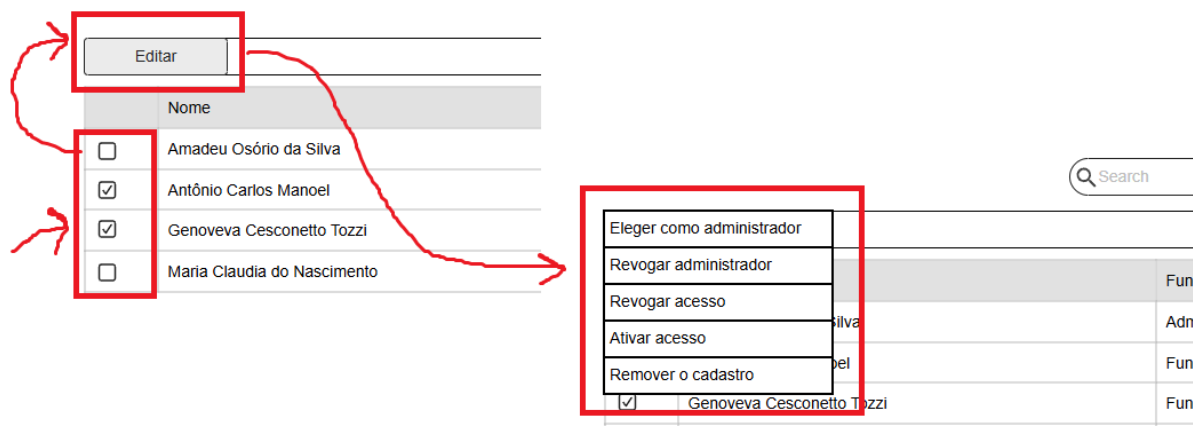
| | Q Search | |
|--|------------------------|---------------|
| | | Novo |
| | Nome | Função |
| | Antônio Carlos Manoel | Administrador |
| | Amadeu Osório da Silva | Funcionário |

A ordenação pode ser feita clicando sobre o título, mas a ordenação padrão é por nome. Deve usar as cores Vermelho para se ordenou e preto se não ordenou.

| | Nome ▲▼ |
|-------------------------------------|-----------------------------|
| <input type="checkbox"/> | Amadeu Osório da Silva |
| <input checked="" type="checkbox"/> | Antônio Carlos Manoel |
| <input checked="" type="checkbox"/> | Genoveva Cesconetto Tozzi |
| <input type="checkbox"/> | Maria Claudia do Nascimento |

Para os requisitos (II, III, IV, V e VI) do administrador deve-se selecionar os funcionários no checkbox de cada funcionário e então utilizar o menu de opções.

¹ Com uma ressalva que o primeiro administrador deve ser cadastrado diretamente por script de instalação.



Cada opção deve ser executada contra os elementos selecionados por uso do checkbox.

1.2.4.2 Interface de cadastro de funcionário

O administrador pode cadastrar outros funcionários, então para acessar a interface abaixo esse teste deverá ser feito. Esta interface pode ser até feita como um Popup.

Nome completo

Username

E-mail:

 @empresa.com.br

☒ Administrador

Criar

Todos os campos são obrigatórios, caso algum campo não seja preenchido então deve-se exibir a mensagem: **Por favor informe NOME DO CAMPO**. Todos os e-mails são corporativos, para testes pode utilizar a plataforma de e-mails yopmail.com. No final do cadastro deve-se exibir a listagem de funcionários e não precisa de ativar conta por e-mail. A ideia é que no primeiro acesso o usuário faça isso (**ATENÇÃO, TEM UMA FALHA AQUI POIS NAO FOI CRIADO O LINK PRIMEIRO ACESSO NA INTERFACE DE LOGIN!!!!**).

1.2.5 Layout da área do Funcionário

O funcionário poderá então criar arquivos .zip com os arquivos de configuração de VPN (cliente), e é natural que também poderá excluir.

| Search | | | | |
|-------------------------------------|---------------|------------|------------|------|
| Remover | | | | Novo |
| Download | Identificador | Data | Validade | |
| <input type="checkbox"/> | AS1AKF1 | 10/10/2024 | 17/10/2024 | |
| <input checked="" type="checkbox"/> | C0F9KLS | 01/01/2025 | 08/01/2025 | |
| <input checked="" type="checkbox"/> | UT9WU01 | 10/01/2025 | 17/01/2025 | |
| <input type="checkbox"/> | YRQ9SAF | 20/05/2025 | 26/05/2025 | |

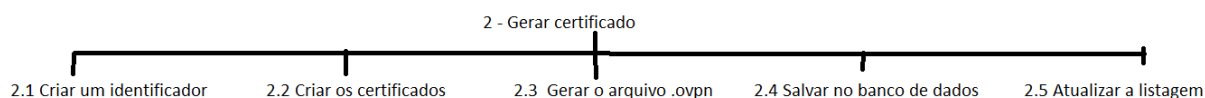
A interface que o funcionário terá acesso deve ter uma lista de arquivos de configuração de VPN que ele já criou, e sempre poderá realizar o download, e também poderá criar quantas configurações quiser.

Toda configuração de VPN terá um identificador único de 7 caracteres podendo ser alfanumérico, deve ser único então deve validar antes de criar o nome. Tem uma data que

foi criada. **Todos estes dados estão no banco de dados.** Também tem que ser possível fazer o filtro por data ou por identificador.

Para remover é simples, o funcionário deve selecionar em um checkbox os arquivos que quer excluir, e então clicar no botão remover. Uma mensagem irá solicitar uma confirmação, afinal arquivos serão excluídos. A mensagem deve questionar: **Você realmente deseja excluir os arquivos C0F9KLS e UT9WU01.** Basta um botão **Sim** (de cor vermelho) e um botão **Não** (de cor verde). **Lembre-se de rodar no servidor um comando para revogar o acesso do certificado especificado antes de excluir do sistema de arquivos.**

Ao clicar no botão Novo o servidor deverá executar uma rotina interna que irá criar os arquivos **.ovpn**, **.crt** e key em um arquivo **.zip**, lembre-se que este arquivo .zip terá o nome do identificador único gerado, conforme já informado.



Como o processo pode demorar, é recomendado que se tenha uma barra mostrando progresso, mas como não se pode mensurar esse tempo, então anime uma barra. **ATENÇÃO: A data de expiração do certificado do cliente deve ser de 7 dias**, então existe uma **VALIDADE**.

O que preocupa é o download, este deve ser realizado com muito critério e por isso não se pode montar URL acessível, ou seja, não podemos forçar uma URL e baixar uma configuração de outra pessoa. Quando fizer o download deve-se ler os bytes de do arquivo .zip e retornar como **application/octet-stream**². Quando configuramos esse tipo de download o arquivo é baixado sempre automaticamente e não cria uma nova URL no histórico.

1.3 Mapa navegacional

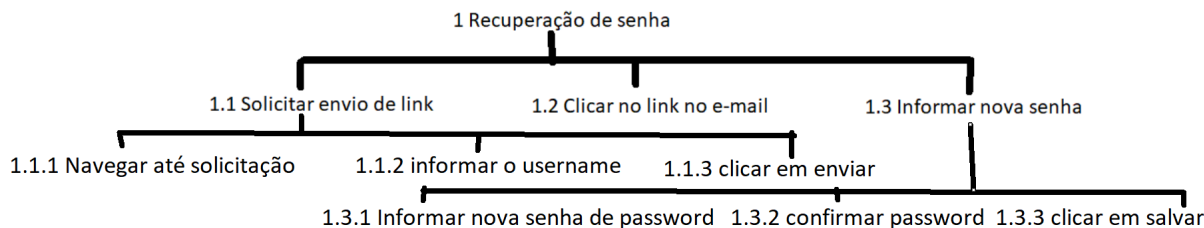
Este sistema engloba ações humanas com ações de scripts, e por isso deve-se atuar para criar rotinas suaves dentro da aplicação.

1.3.1 Redefinição de senha

Tanto para recuperar uma senha, pois o usuário esqueceu quanto para criar uma senha no primeiro acesso, o usuário deverá seguir uma série de passos, que envolve telas do próprio sistema quanto às telas de seu e-mail corporativo. Abaixo temos o HTA detalhado para redefinição de senhas.

² Neste link você encontra um exemplo em PHP:

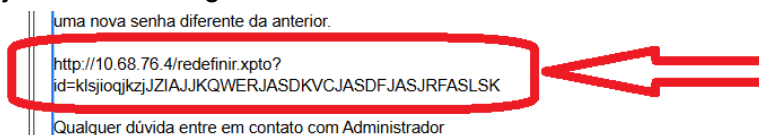
<https://dev.to/accreditly/streaming-large-files-with-php-to-save-memory-4nmk> se escolher Java, converta o exemplo.



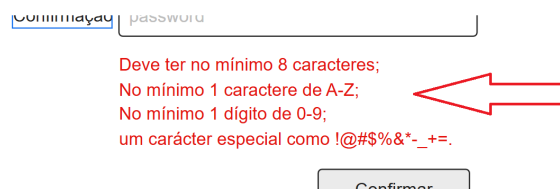
O 1.1 seria então o momento que na tela de Login se clica no link “Redefinir uma Senha”, então será levado para a interface “Solicitação de Link”, nesta tela é importante que ele informe seu Usuário (username de login na VPN).



Conforme já descrito é enviado um e-mail, acontece que deve ser um e-mail corporativo sendo enviado para outro corporativo. O link deve estar sempre visível mas não manda como link, ou seja, não use a tag <a>.



Depois será redirecionado para uma interface de definição de senha, veja, as regras de senha devem estar nesta tela, não coloque estas regras na tela pública pois facilita uma possível tentativa de invasão. A pessoa então deve informar o usuário e a senha nova, confirme sempre, se o usuário informar a mesma senha que já tem, deve-se informar a mensagem: **A nova senha não pode ser igual a senha anterior**. Estas regras estão definidas na interface chamada “Nova Senha”.

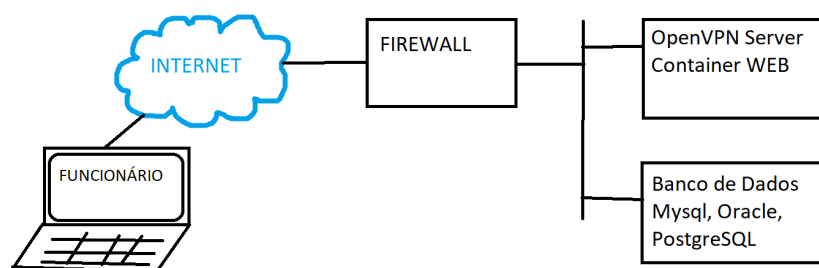


Não precisa criar nenhum flag nestes itens, e a senha deve ser exibida com * para evitar possível captura de tela.

Atenção, o usuário deve ser redirecionado para interface de Login, pois se você jogar ele para dentro do sistema nesta etapa, e no futuro ele perceber que errou a senha, ele aciona a TI dizendo que foi invadido. Então já joga ele agora nesta tela de login para ele perceber agora se ele fez direitinho a redefinição de senha.

1.4 Disposição dos serviços na Rede e Regras

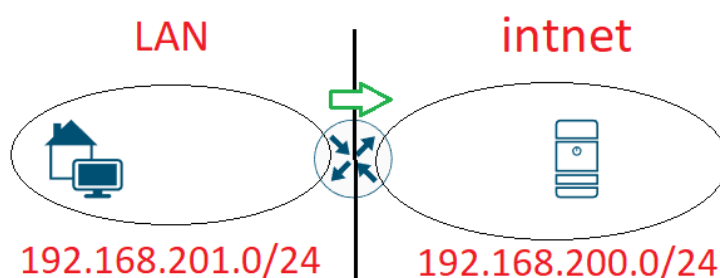
Com o objetivo de ter um serviço seguro é importante que se faça o uso de um Firewall entre o servidor OpenVPN e a Internet, e por questões de boas práticas isola-se o banco de dados da aplicação. Para fins de facilidade será permitido que o Container WEB esteja no mesmo servidor do OpenVPN, mas deve-se aplicar as boas práticas de segurança segundo o **OWASP Top 10**.



Este Firewall deve permitir que as portas sejam retransmitidas para o OpenVPN, as portas devem ser (devem ser aplicadas no firewall):

| Porta | Protocolo | Serviço | Descrição |
|-------|-----------|---------------|---|
| 80 | TCP | Container WEB | Permitir para fazer redirecionamento com rewrite para 443 |
| 443 | TCP | Container WEB | Interface WEB que deverá responder às requisições do Browser. |
| 1194 | UDP | OpenVPN | Porta do serviço VPN para que clientes possam se conectar |

Todos os outros protocolos devem ser bloqueados se forem originados na Internet com destino aos servidores internos, conforme já visto. Para aumentar a segurança, devemos aplicar uma regra que só permitirá acesso a porta 22 do servidor OpenVPN para quem está na rede **192.168.200.0/24**. Ou seja, só poderá acessar o SSH do servidor OpenVPN se estiver na empresa (fisicamente).



Para o servidor de Banco de Dados, também deve-se aplicar a mesma regra.