PCI-DSS

CENTRO DE PESQUISA E DESENVOLVIMENTO TECNOLÓGICO EM INFORMÁTICA E ELETROELETRÔNICA DE ILHÉUS

Relembrando

Objetivo & Investigação

Informações & Coleta

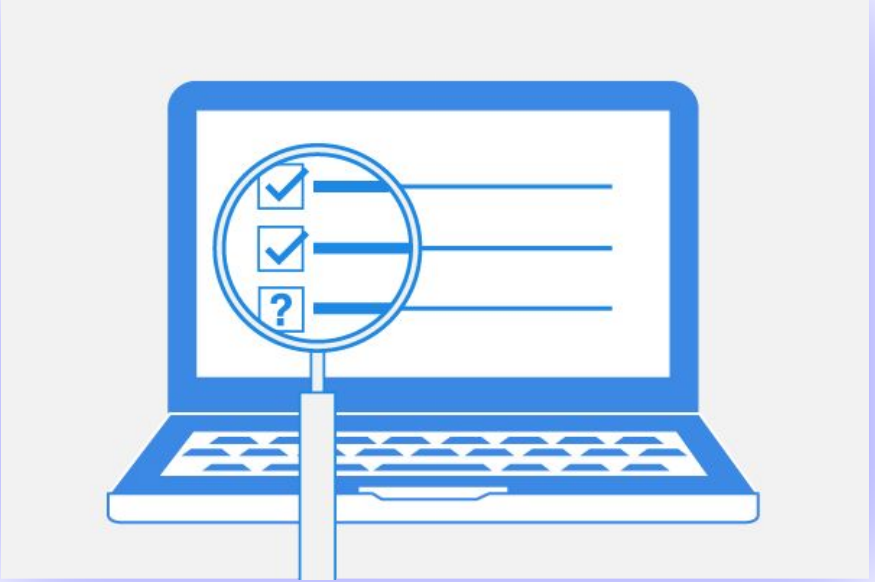
Análise

1. Captcha e fatores de respostas.

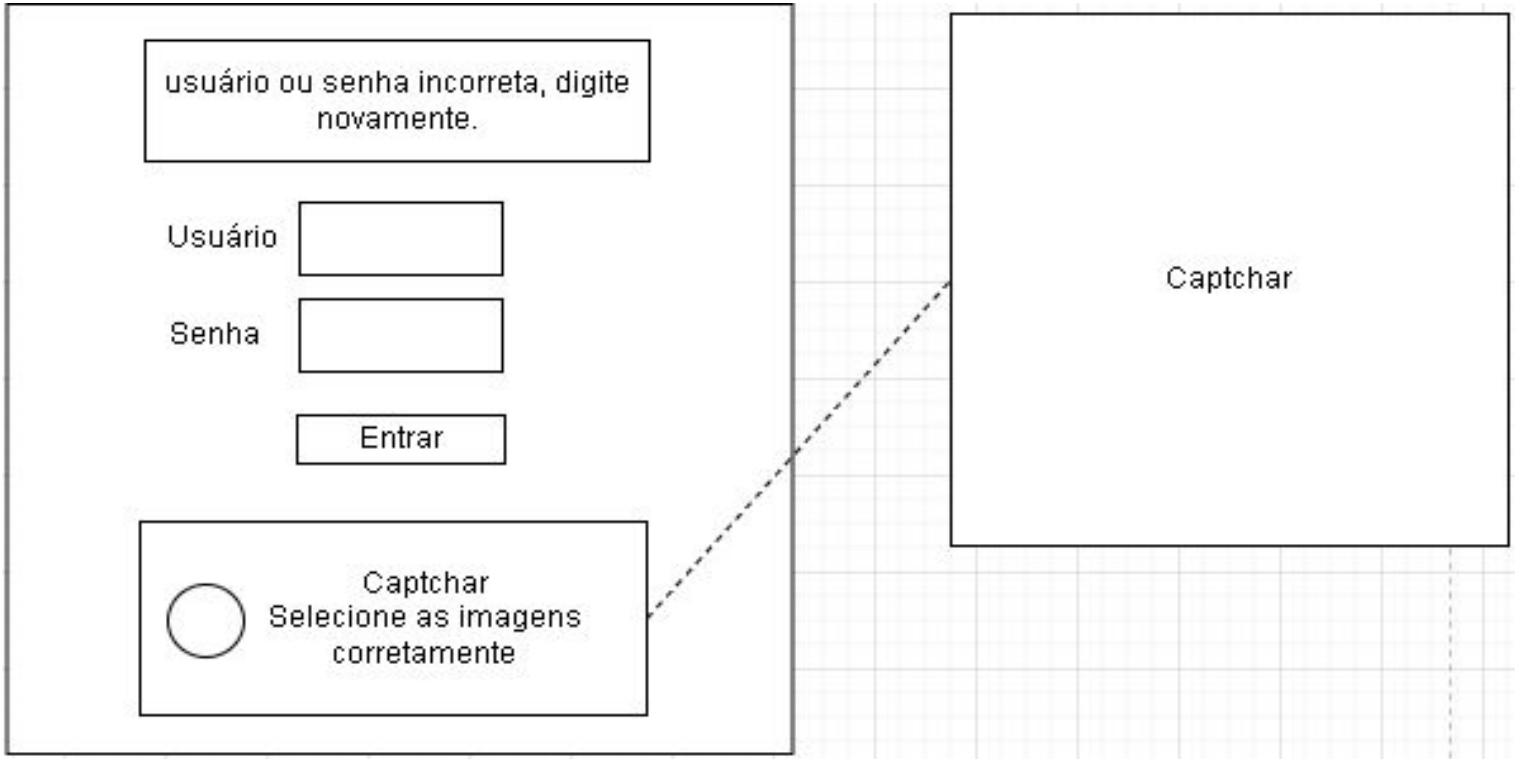
1.1 Fator de resposta para 1 tentativa incorreta: Apresentar *Captcha*.

1.2 Fator de resposta para 3 tentativas incorretas: Aplicar *time out.*

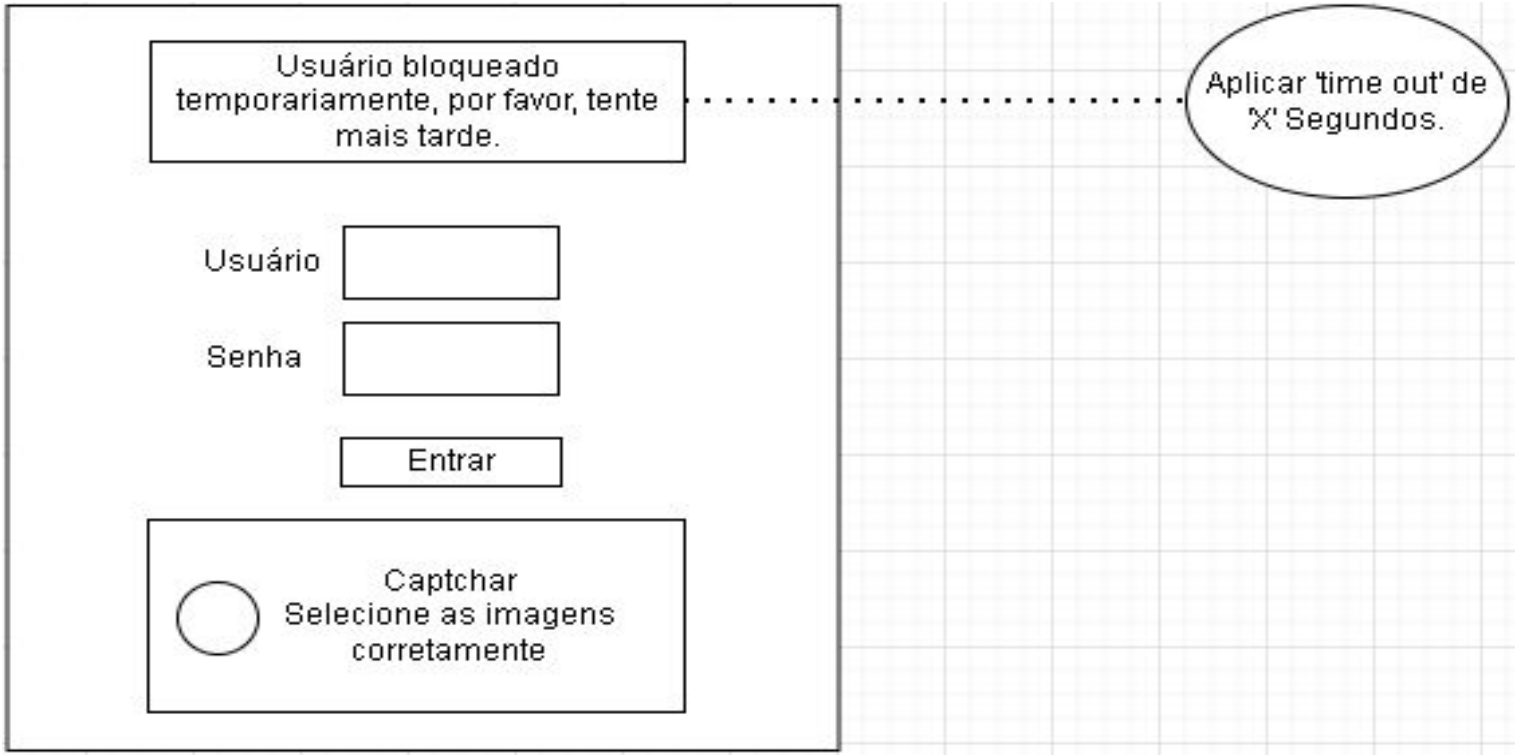
1.3 Fator de resposta para 5 tentativas incorretas: Aplicar bloqueio.



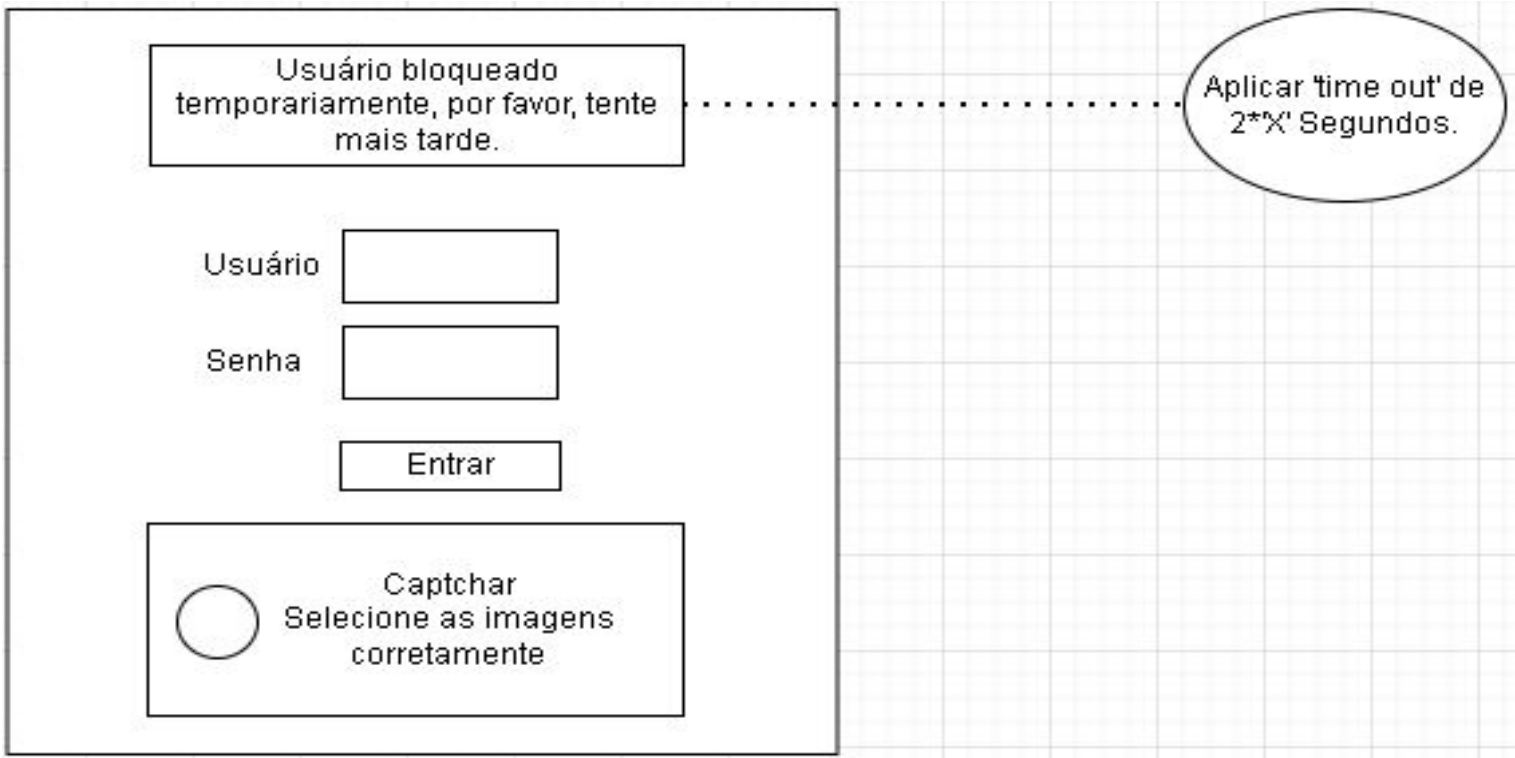
Primeira interação



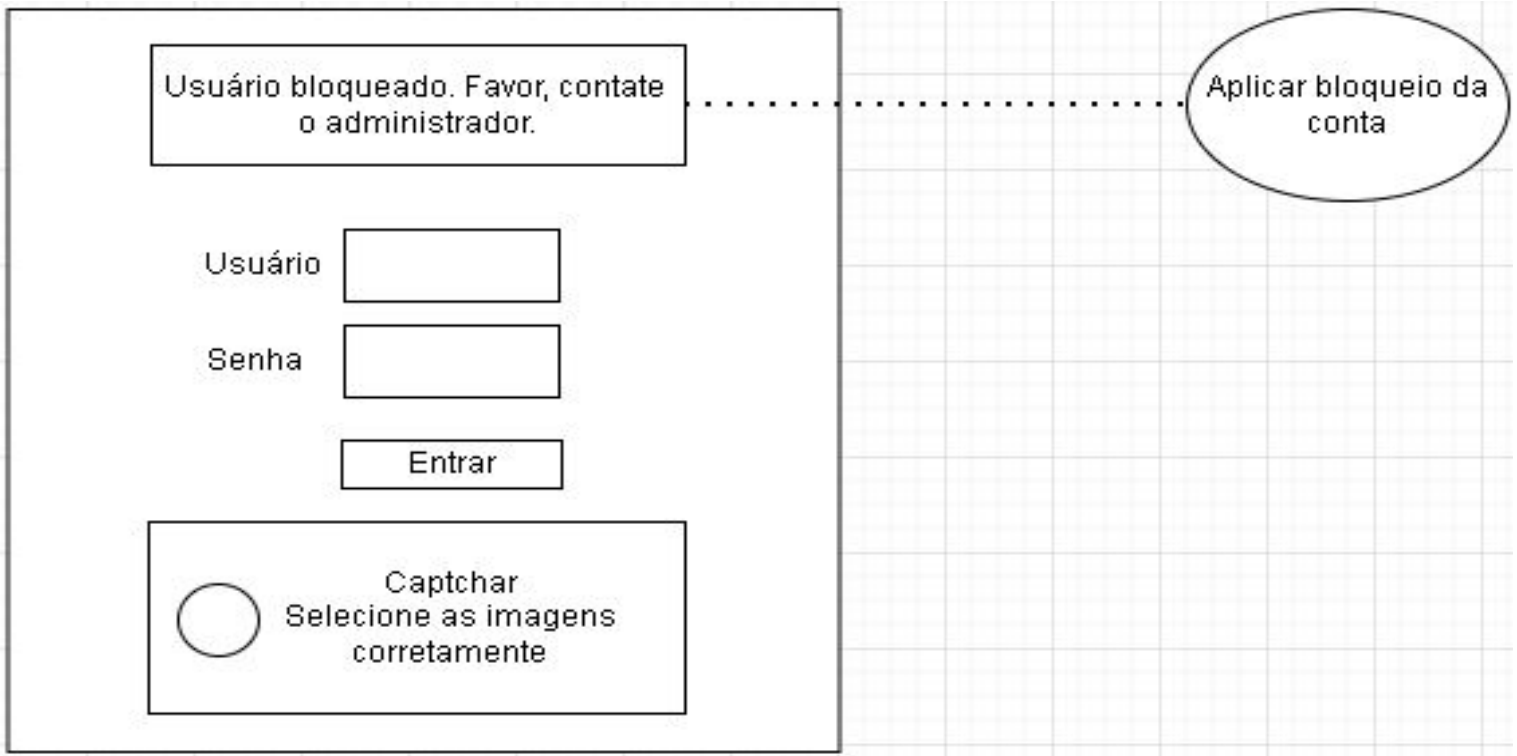
Terceira interação



Quarta interação



Quinta interação



2. Autenticação Forte

A senha forte é constituída por letras maiúsculas, minúsculas, números e caracteres especiais.

EM QUANTO TEMPO DESCOBRIRIAM SUA SENHA?

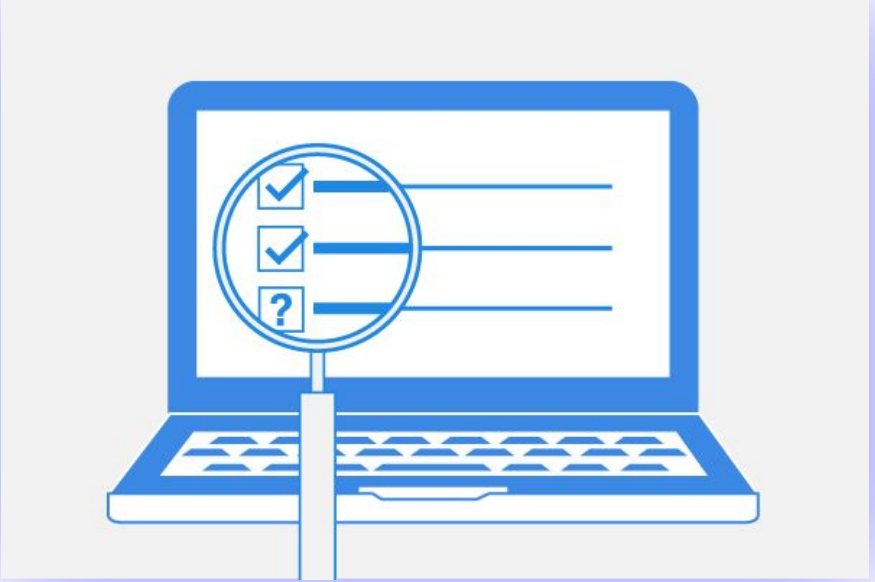
TAMANHO DA SENHA	SÓ NÚMEROS	MIX DE LETRAS MINÚSCULAS E MAIÚSCULAS	MIX DE LETRAS MINÚSCULAS, MAIÚSCULAS E NÚMEROS	MIX DE LETRAS MINÚSCULAS E MAIÚSCULAS, NÚMEROS E SÍMBOLOS
Pequena (3 a 5 caracteres)	INSTANTANEAMENTE	INSTANTANEAMENTE	ATÉ 3 SEGUNDOS	ATÉ 10 SEGUNDOS
Média (6 a 10 caracteres)	ATÉ 40 SEGUNDOS	ATÉ 169 DIAS	ATÉ 1 ANO	ATÉ 928 ANOS
Grande (12 a 15 caracteres)	ATÉ 46 DIAS	ATÉ 28 MILHÕES DE ANOS	ATÉ 1 BILHÃO DE ANOS	ATÉ 2 TRILHÕES DE ANOS

3 Regra para modificação de senha

Não permitir a criação de uma nova senha que seja igual a qualquer uma das últimas quatro ou cinco senhas utilizadas anteriormente.

4.0 Rastreie e monitore todo o acesso(logs)

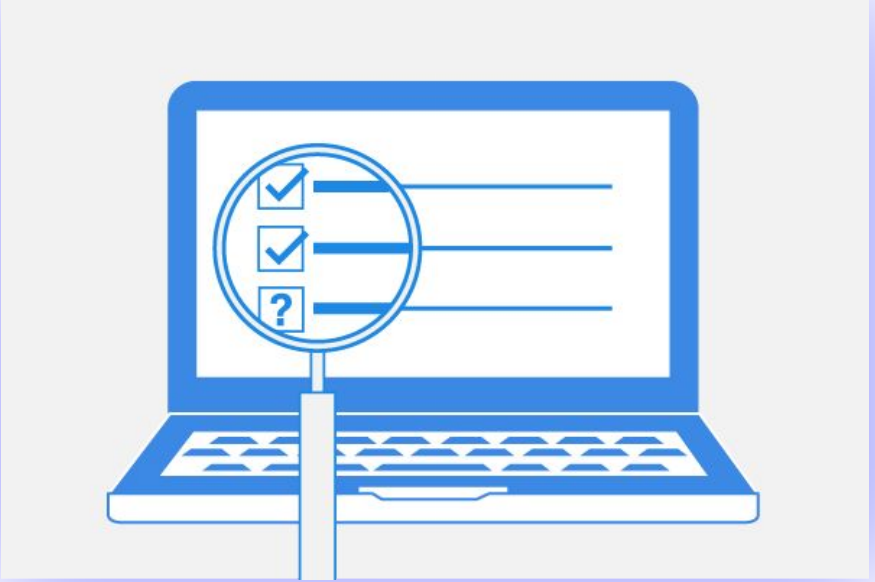
O uso de mecanismos de log é fundamental para prevenir, detectar e minimizar ameaças à segurança de dados. Quando as atividades relacionadas aos usuários do sistema não são registradas, uma possível violação não pode ser identificada.



4.1 Informações mínimas do eventos de log

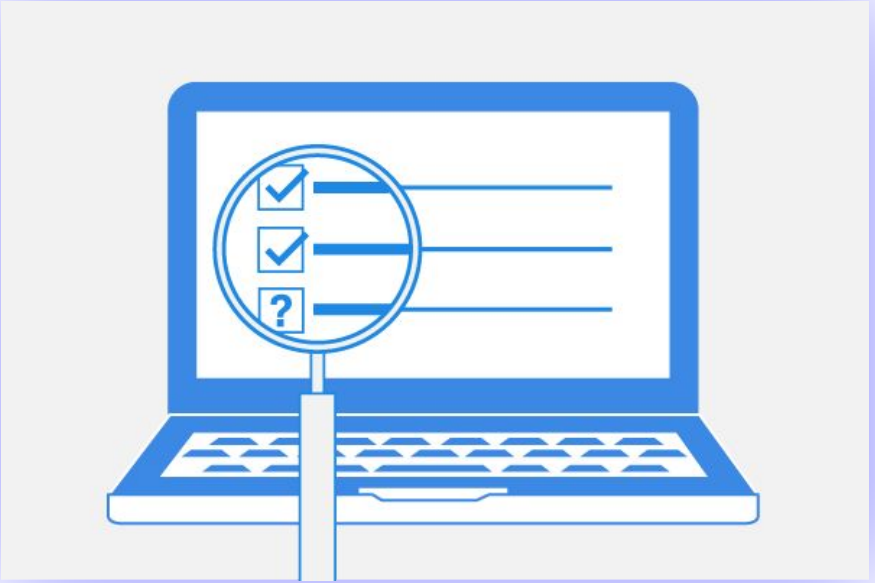
1. ID do usuário
2. Tipo de evento
3. Data e hora
4. Indicador de sucesso ou falha
5. A Origem do Evento
6. Identidade ou nome dos dados afetados, recurso, componente do sistema

É essencial que os eventos sejam registrados com essas informações para identificação rápida e fácil de qualquer violação de dados, quem, quando, onde, o quê e como fazê-lo.



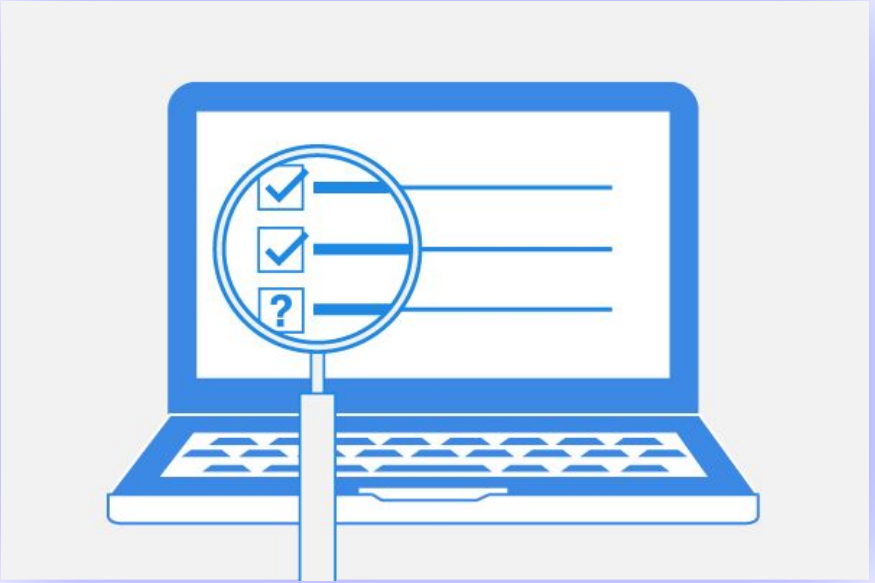
4.2 Eventos de logs não podem ser alterado

A alteração de logs pode representar uma séria ameaça à segurança, pois, em caso de violação das informações, nenhum dado real do log será encontrado e não será possível identificar o responsável pelo real motivo. Por esse motivo, os arquivos de log devem ser armazenados de forma que não possam ser alterados.



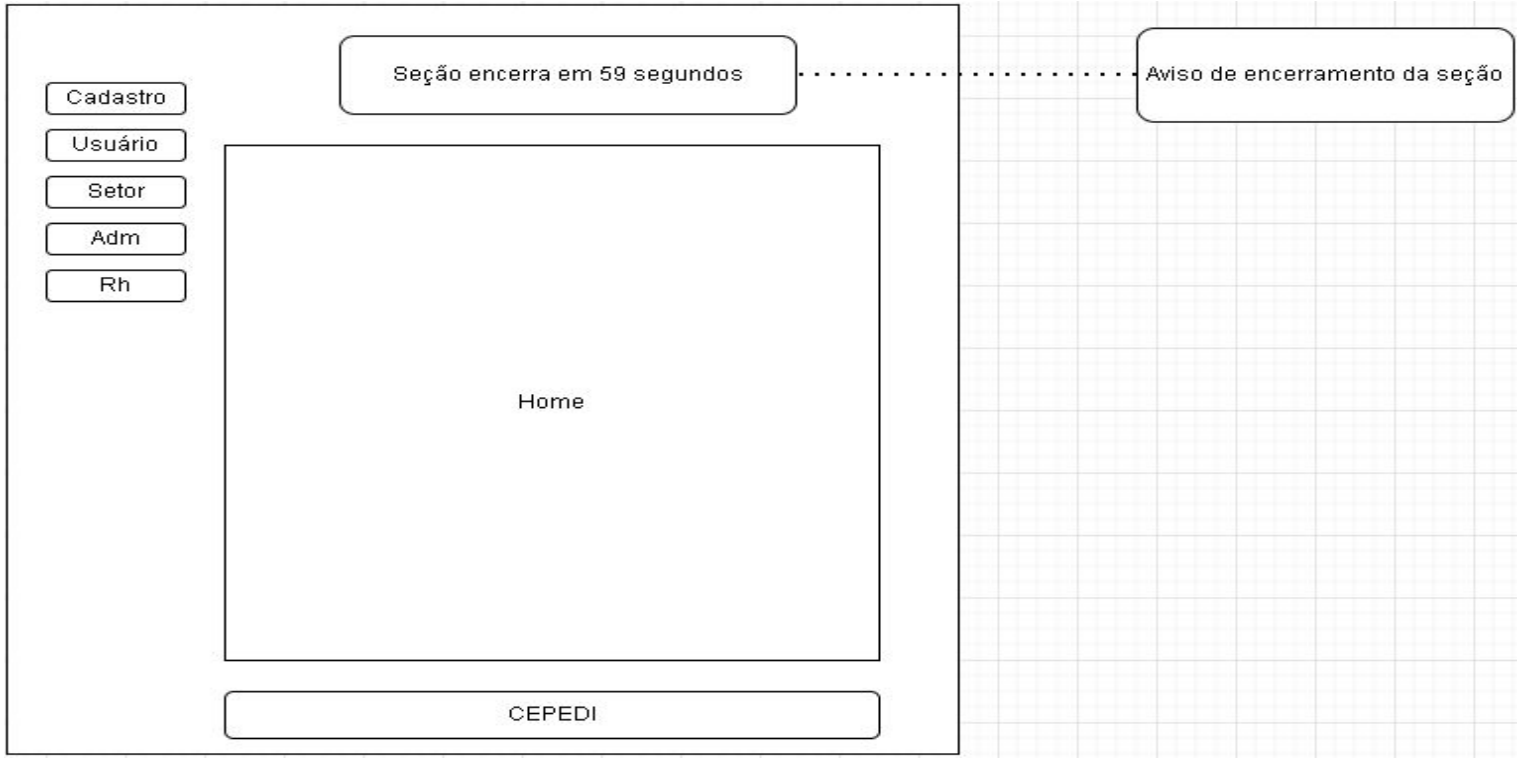
4.3 Armazenamento das informações

Reter o histórico de log por pelo menos um ano e ter pelo menos três meses de dados prontos para análise.



4.4 Tempo Limite de inatividade

Os recursos de tempo limite de inatividade do sistema / seção foram definidos para 15 minutos.


Seção encerra em 59 segundos
Aviso de encerramento da seção
Cadastro
Usuário
Setor
Adm
Rh
Home
CEPEDI

Sobre os sistemas do CEPEDI

Verificamos dezoito sistemas do CEPEDI, onde constatamos que cem por cento dos sistemas precisam de 1 ou mais modificações a serem feitas.

Plano Estratégico

Os núcleos do CEPEDI tem diferentes metodologias, ferramentas e linguagens de programação utilizadas. A forma de implementação ficará na responsabilidade do núcleo, desde que contemple perfeitamente os requisitos mínimos PCI-DSS. A sugestão é criar tarefas de melhoria e correção, indicando como deve ser feito e, obviamente, monitorando a construção para que assim, possamos chegar ao objetivo final.

Concluindo