




Ministério da Justiça

Projeto: SINDEC

Nota Técnica

MJ	e-Certidão - Nota Técnica	
-----------	----------------------------------	--

Revisão	Descrição	Autor	Data
1.0	Construção do documento	Israel Branco	21/05/2020

1 Sumário

- 2 Introdução.....4
- 3 Apresentação do cenário atual.....5
 - 3.1 Tecnologias utilizadas.....6
 - 3.2 Modelagem de dados.....7
 - 3.3 Organização do projeto.....9
- 4 Análise técnica.....10
 - 4.1 Padrão de codificação.....10
 - 4.2 OWASP ZAP.....12
 - 4.3 UX - User experience.....14
- 5 Conclusão.....15

2 Introdução

Este documento visa reportar o resultado da análise efetuada no sistema SINDEC. Para este estudo foram desconsiderados todo o contexto negocial ao qual a ferramenta está inserida juntamente com o ambiente ao qual a ferramenta opera em ambiente produtivo, sendo analisado puramente questões que tangem a qualidade de código, padrões de codificação, modelo relacional de banco de dados e concepção arquitetural.

3 Apresentação do cenário atual

Esta sessão ira descrever a arquitetura, tecnologias, frameworks e dependências que compõe a base da aplicação. Para esta análise fora utilizado a tag ctis-nota-tecnica-20200521 gerada a partir da branch stable em 21/0/2020 (<https://gitlab.mj.gov.br/cgsis/sindec/tree/ctis-nota-tecnica-20200521>).

O projeto SINDEC esta composto por 5 projetos mesclados entre tecnologia ASP (Sindec, SindecAtendimentoWEB, SindecConsulta e SindecRelatorios) e tecnologia PHP (FluxoMinucupalizacao, ImportarAtualizarCEP, SindecDownload, SindecPDF)

Os projetos construídos com tecnologia ASP foram criados para a trabalhar em ambiente web sob protocolo utilizando banco de dados MySQL com conexão ODBC, implantada em servidor de aplicação Microsoft IIS com suporte a aplicações ASP.

Os projetos construídos com tecnologia PHP tais como FluxoMunicipalizacao e ImportarAtualizarCEP foram construídos para trabalhar de forma pontual e isolada com com executável *.bat*, funcionando como aplicações de simples execução para atualização de dados em tabelas de banco de dados. Os demais foram construídos para operar em ambiente WEB.

Com exceção do projeto Sindec (ASP), não há evidências de execução dos demais projetos em ambiente WEB e por estas razões manteremos este projeto como foco desta análise.

3.1 Tecnologias utilizadas

Esta sessão descreve as tecnologias, frameworks e principais bibliotecas utilizadas na construção dos projetos, descrevendo versões e propósitos de utilização.

Nome	Versão	Utilização	Observação
ASP	3	Linguagem de programação.	
ODBC	x	Conexão com banco de dados.	
MySQL	x	Banco de dados.	
IIS	7	Servidor de aplicação Microsoft.	

3.2 Modelagem de dados

O sistema SINDEC utiliza 3 bases de dados sendo elas SINDEC, SINDECATENDIMENTOWEB e CEP. Suas estruturas são compostas por 109 tabelas, 9 tabelas e 5 tabelas respectivamente.

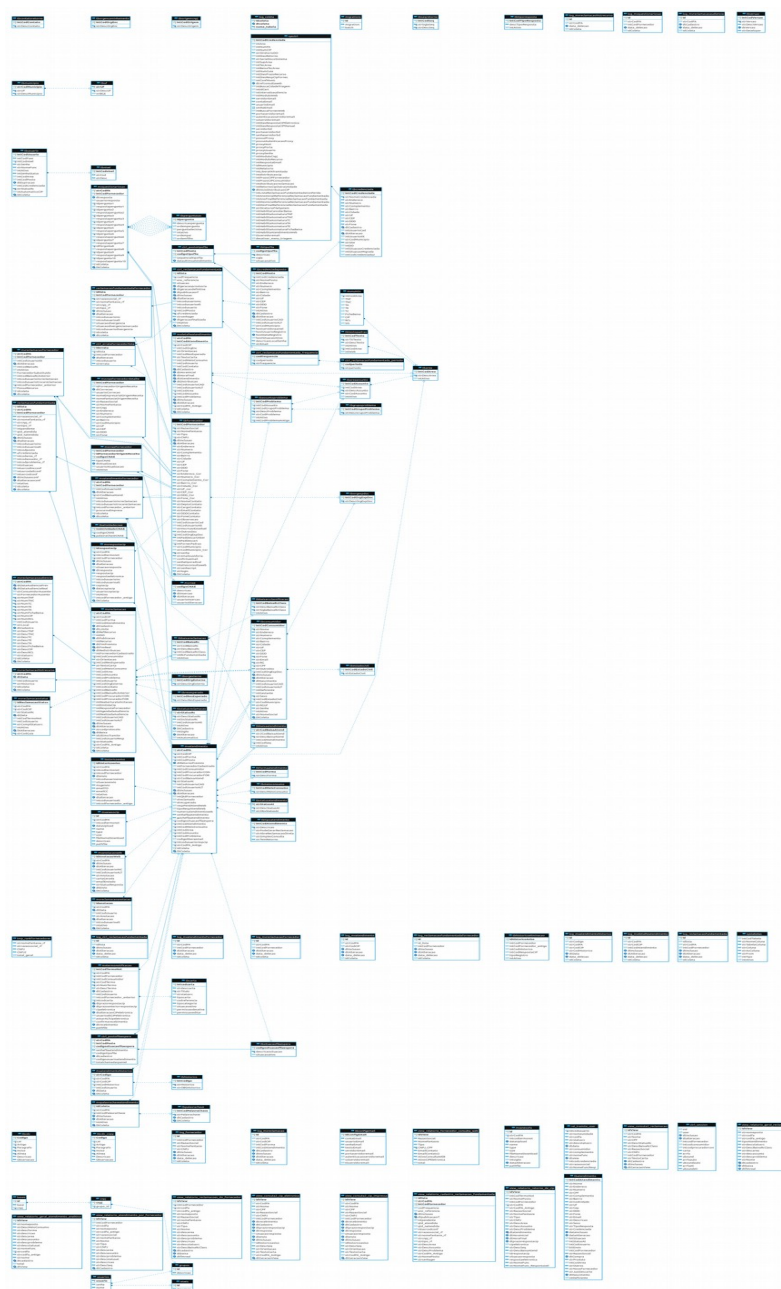


Figura 1: MER - Sindec

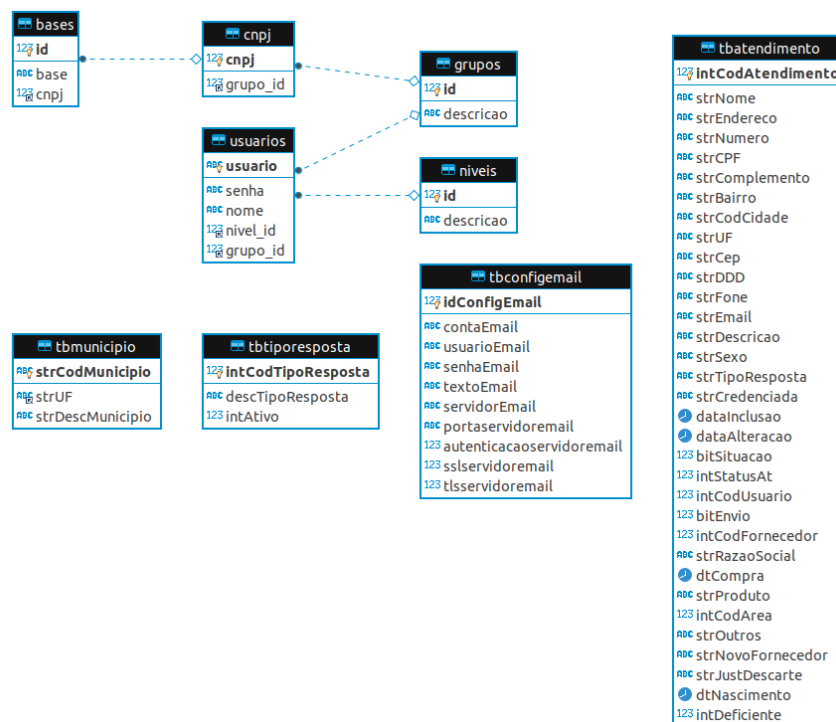


Figura 2: MER - SindecAtendimentoWEB

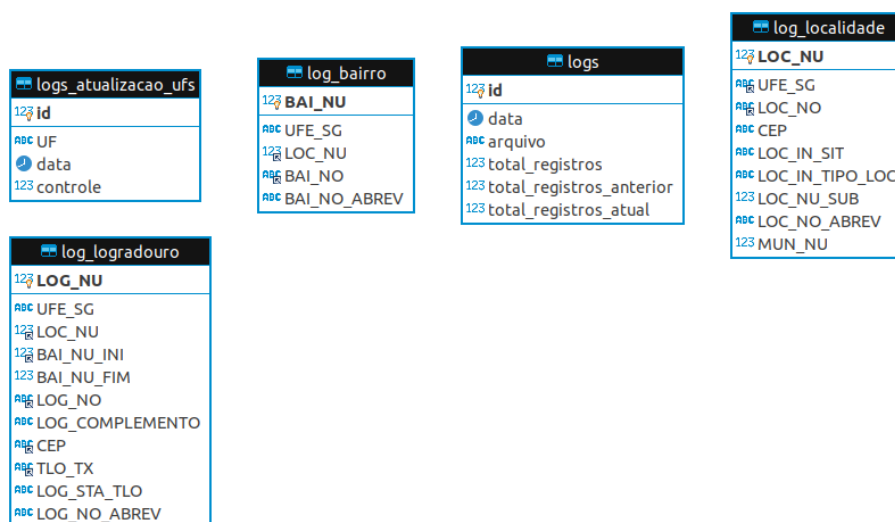


Figura 3: MER - CEP

3.3 Organização do projeto

O projeto tem organização com segregação de diretórios por funcionalidade/tipos de arquivos, há no diretório raiz deste projeto arquivos que aparentam serem compartilhados por demais funcionalidades.

Os diretórios que tangem especificamente sobre as funcionalidades possuem consigo arquivos de várias extensões, tais como arquivos javascript, folhas de estilo, arquivos de imagens e páginas ASP. Arquivos com estas extensões com exceção de arquivos ASP são encontrados em diretórios específicos que partem do diretório raiz.

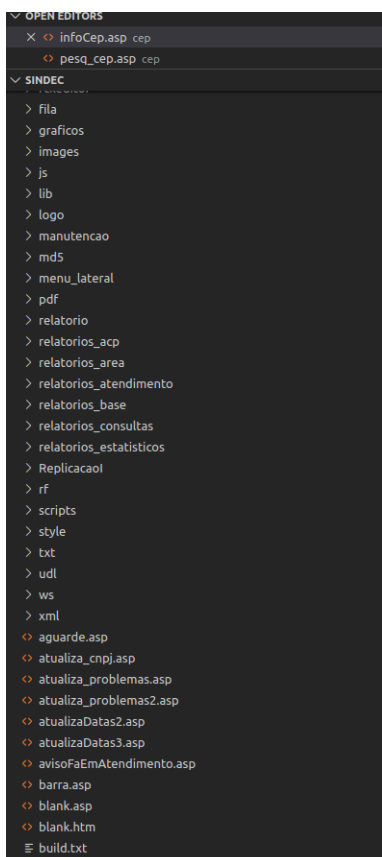


Figura 5: Organização do projeto

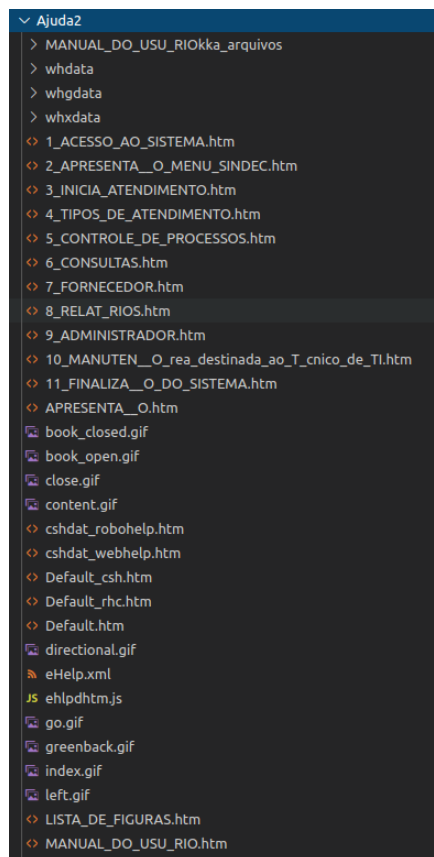


Figura 4: Organização dos subdiretórios

4 Análise técnica

Este tópico descreve a ferramenta do ponto de vista técnico, tanto nos aspectos de codificação, análise estática de código, análise de vulnerabilidade de dependências e particularidades de implementação.

4.1 Padrão de codificação

Tratando-se de tecnologia obsoleta não há ferramentas gratuitas que efetuem análise estática de código para a tecnologia ASP 3.0, as evidências demonstradas a seguir serão apresentadas com base em análise amostral de código.

O código do projeto não apresenta boa segregação e não há reaproveitamento de código com a utilização de includes de artefatos, há maioria das páginas apresentam grande quantidade de código sendo este, embaralhado entre funções ASP, JavaScript e HTML. A imagem a seguir representa o que foi relatado e encontramos este cenário em boa parte da aplicação.

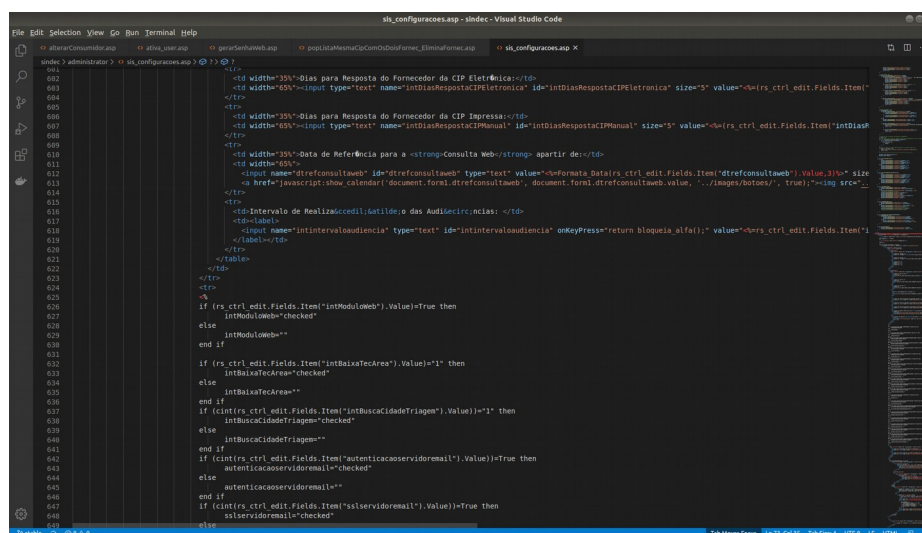


Figura 6: Mistura de código HTML/ASP

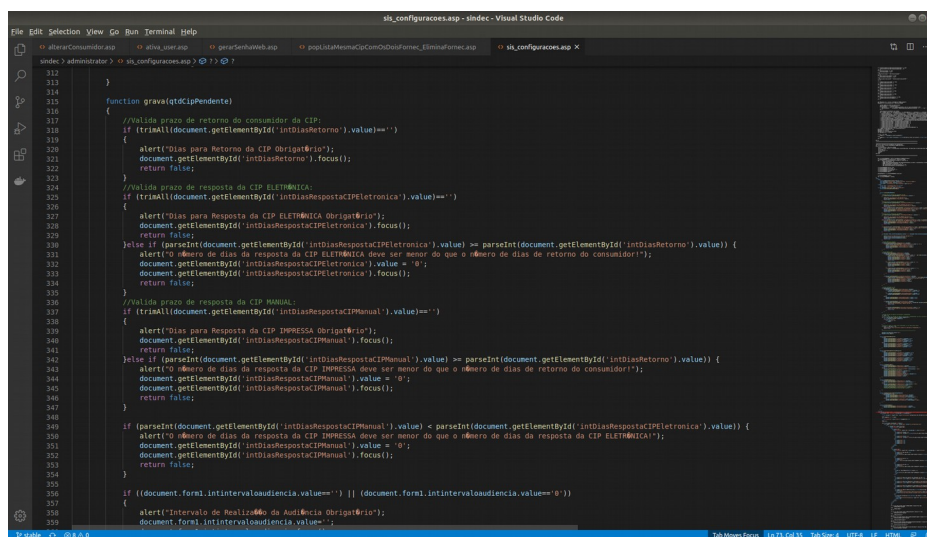


Figura 7: Mistura de código JavaScript/HTML/ASP

Código macarrônico ou código espaguete é o termo utilizado para descrever o *AntiPattern* que não segue regras de programação estruturada, mal organizada, com desvios e códigos difíceis de analisar. Este AntiPattern descreve o código produzido para o sistema SINDEC, a mistura de tecnologias ao longo das páginas e a altíssima complexidade ciclométrica dificultam a testabilidade funcional do sistema e as manutenções corretivas.

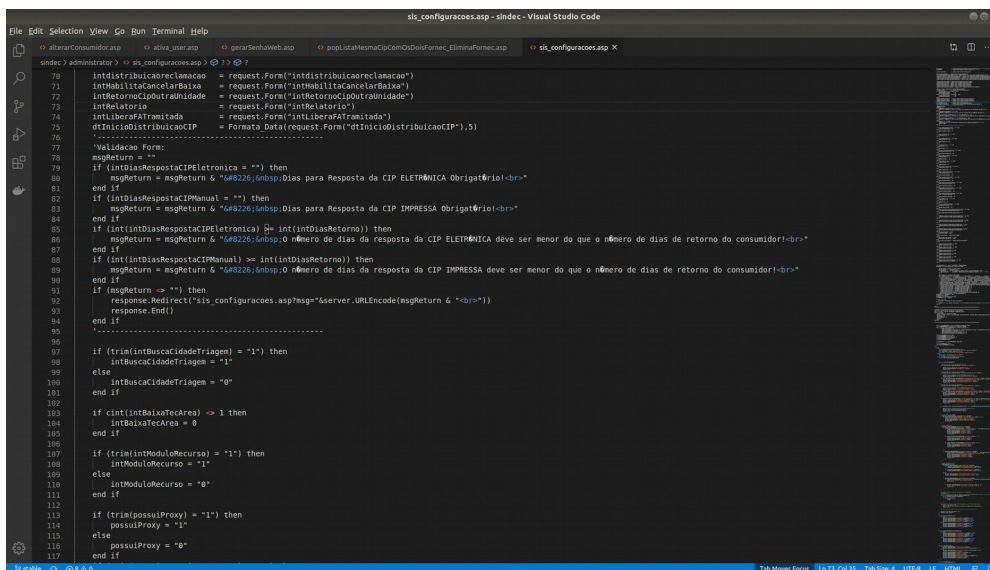
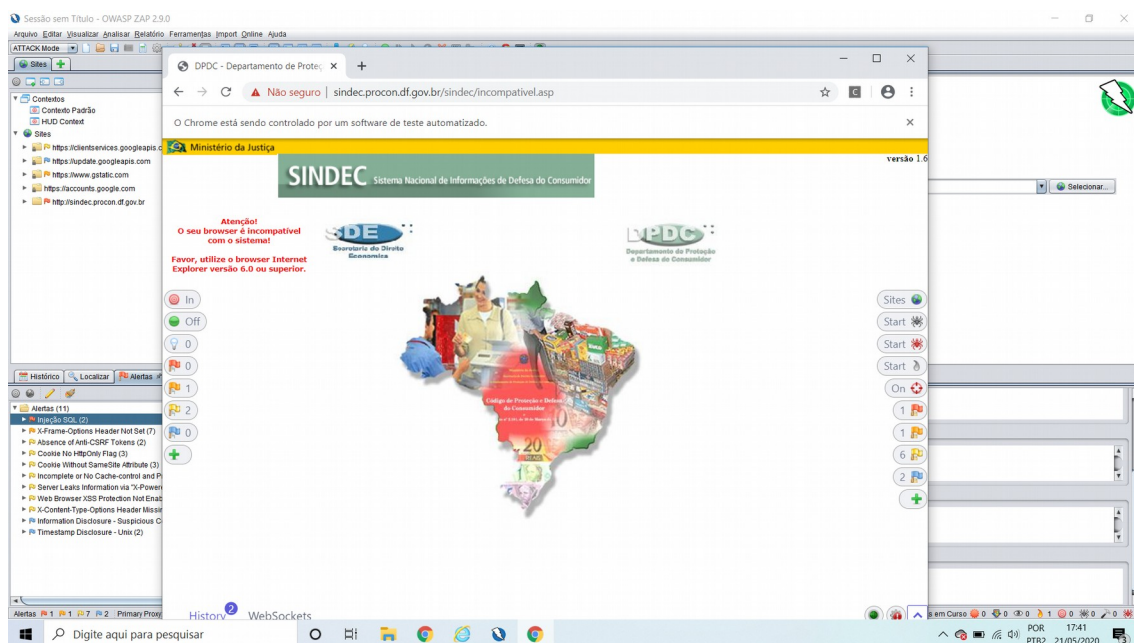


Figura 8: Complexidade ciclométrica

4.2 OWASP ZAP

Ferramenta funciona como scanner de segurança, utilizada para realização de testes de vulnerabilidade de aplicações WEB e atualmente trata-se de um dos projetos mais ativos na comunidade de software livre.



O detalhamento desta análise está classificada em:

- 1 vulnerabilidade de severidade alta;
- 2 vulnerabilidades de severidade média;
- 8 vulnerabilidades de baixa média;
- 4 vulnerabilidades a nível informativo;

Os detalhes deste relatório estão disponíveis no anexo I deste documento. Vale ressaltar que fora encontrado nesta análise potencial risco de ataque por injeção de SQL, sendo este classificado dentro dos top 10 das falhas de vulnerabilidade mais críticas em



aplicações WEB.

```

sis_configuracoes.asp - sindec - Visual Studio Code
File Edit Selection View Go Run Terminal Help
<-- alteraConsumidor.asp <-- ativa_user.asp <-- geraSenhaWeb.asp <-- popListaMesmaCipComOsDolsFornec_EliminaFornec.asp <-- sis_configuracoes.asp X
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262

'Valida update da senha do usuario proxy:
UPD_proxySenha = " , proxySenha=null
if (proxySenha <> "" and not isempty(proxySenha) and not isnull(proxySenha)) then
    UPD_proxySenha = " , proxySenha=" & ReplaceEmailHash(getHash(proxySenha), "C", "", "") & " "
end if

'Atualizacao dos parametros do sistema:
SQL = "UPDATE sysctrl SET intDiasRetorno = " & intDiasRetorno & ", intSupArea = 1, intTecArea = 1, intBaixaTecArea = " & intBaixaTecArea & "
", intDiasPrazoRecurso = " & intDiasPrazoRecurso & ", dtRefConsultWeb = " & dtRefConsultWeb & ", intBuscaCidadeTriagem = " & intBuscaCidadeTriagem & "
", intIntervaloAudencia = " & intIntervaloAudencia & ", intDiasRespostaCIPeletronica = " & intDiasRespostaCIPeletronica & ", intDiasRespostaCIPManual = " & intDiasRespostaCIPManual & "
", intModuloCnpj = " & intModuloCnpj & ", possuiProxy = " & possuiProxy & ", possuiAutenticacaoProxy = " & possuiAutenticacaoProxy & ", proxyHost = " & proxyHost & "
", proxyPort = " & proxyPort & ", proxyUser = " & proxyUser & ", intModuloRecurso = " & intModuloRecurso & ", intRespostaEmail = " & intRespostaEmail & "
", intDistribuidoCIP = " & intDistribuidoCIP & ", intPrazoCIPFornecedor = " & intPrazoCIPFornecedor & ", intPrazoCIPConsumidor = " & intPrazoCIPConsumidor & ", intDistribuidoCIP = " & intDistribuidoCIP & "
", intRetornoCIPoutraUnidade = " & intRetornoCIPoutraUnidade & ", intRelatorio = " & intRelatorio & ", intLiberaATramitada = " & intLiberaATramitada & ", dtInicioDistribuidoCIP = " & dtInicioDistribuidoCIP & "
", intAnoInicialReferenciaReclamacaoFundamentada = " & intAnoInicialReferenciaReclamacaoFundamentada & ", intRespostaReferenciaReclamacaoFundamentada = " & intRespostaReferenciaReclamacaoFundamentada & "
", intAnoFinalReferenciaReclamacaoFundamentada = " & intAnoFinalReferenciaReclamacaoFundamentada & ", intMesInicialReferenciaReclamacaoFundamentada = " & intMesInicialReferenciaReclamacaoFundamentada & "
", intHabilitaAssinaturaTNC = " & intHabilitaAssinaturaTNC & "
", intHabilitaAssinaturaTNC6 = " & intHabilitaAssinaturaTNC6 & "
", intHabilitaAssinaturaTE = " & intHabilitaAssinaturaTE & "
", intHabilitaAssinaturaTA = " & intHabilitaAssinaturaTA & "
", intHabilitaAssinaturaTE6 = " & intHabilitaAssinaturaTE6 & "
", intHabilitaAssinaturaFichaBaixa = " & intHabilitaAssinaturaFichaBaixa & "
", WHERE intCodCredenciada = " & intCodCredenciada & ""

MM_Update_ctl.CommandText = SQL
MM_Update_ctl.Execute
MM_Update_ctl.ActiveConnection.Close
set MM_Update_ctl = nothing

if (Err <> 0) then
    msgReturn = "Problemas ao salvar parâmetros"
else
    msgReturn = "<span class='txtsucesso'><strong>Parâmetros salvos com sucesso</strong></span>"
end if

```

Figura 9: Código SQL nas páginas ASP

4.3 UX – User experience

A ferramenta não apresenta padronização de interfaceamento gráfico compatível com as especificações do Governo Federal (<http://epwg.governoeletronico.gov.br/guia-administracao>), também não há compatibilidade com outros navegadores que diferem do Internet Explorer que mesmo sendo em versões superiores a 6, precisam ser executados em modo de compatibilidade.

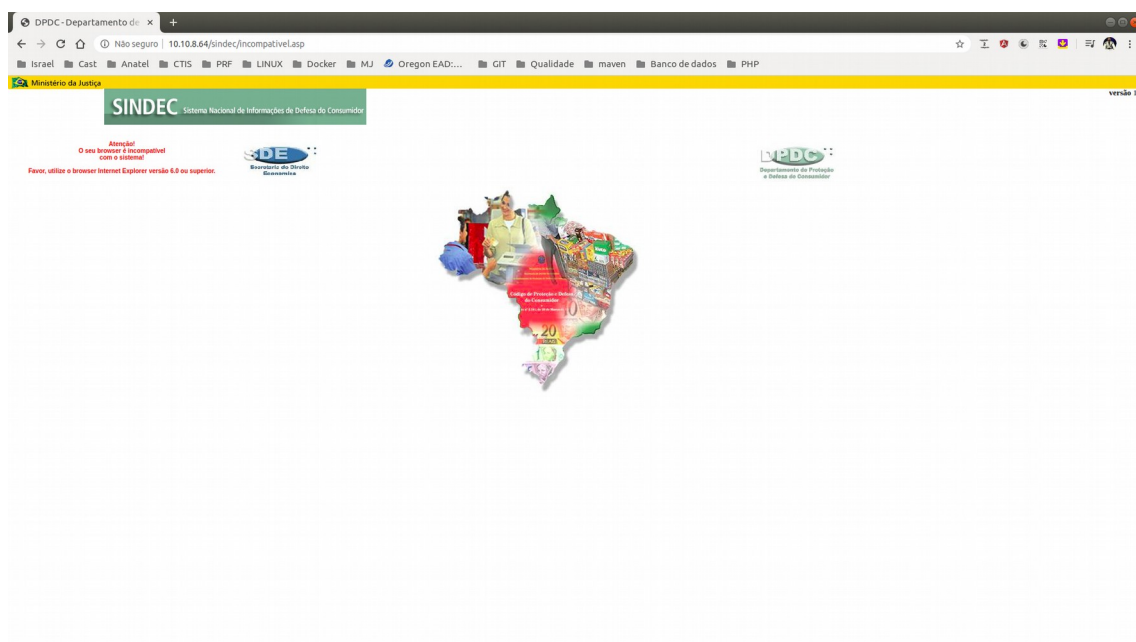


Figura 10: Incompatibilidade com navegadores

Após logar na ferramenta utilizando o navegador Internet Explore a aplicação encerra o navegador e abre a aplicação em um pop up, exigindo assim que os mesmos estejam desbloqueados.

5 Conclusão

A aplicação não apresenta boas práticas em sua construção, também não apresenta boa apresentação visual e boa usabilidade.

Por estar concebida com tecnologia defasada, há dificuldades na manutenção do ambiente produtivo para hospedagem e escalabilidade da mesma.

Há extrema complexidade ciclomática nas páginas que compõe o contexto da solução, esta complexidade certamente dificulta os testes funcionais e as manutenções corretivas e evolutivas.

Uma vez que não atende aos padrões de codificação, usabilidade, manutenção e segurança da informação, não recomenda-se a manutenção da aplicação em ambiente produtivo, sugere-se que a mesma seja reescrita utilizando a arquitetura de referência adotada para as aplicações WEB do Ministério da Justiça respeitando as características negociais hoje aplicados e as necessidades de evolução do contexto negocial da solução.