



Departamento de Polícia Rodoviária Federal

Projeto: Siadi

Nota Técnica

DPRF	DPRF Segurança - Nota técnica	
-------------	--------------------------------------	--

Revisão	Descrição	Autor	Data
1.0	Construção do documento	Israel Branco	27/05/2020

1 Sumário

2 Considerações iniciais.....	4
3 Apresentação do cenário atual.....	5
3.1 Tecnologias utilizadas.....	8
4 Análise técnica.....	9
4.1 SonarQube.....	9
4.2 OWASP Dependency Check.....	10
4.3 OWASP ZAP.....	11
4.4 Estrutura do projeto.....	13
4.5 Manutenibilidade de código.....	14
4.6 Confiabilidade.....	19
4.7 Performance e estabilidade.....	20
5 Recomendações.....	21

2 Considerações iniciais

Este documento visa reportar o resultado da análise efetuada na aplicação SIADI. Para este estudo foram desconsiderados todo o contexto negocial ao qual a ferramenta está inserida, também foram desconsideradas o ambiente ao qual a ferramenta esta operando sendo analisado puramente questões que tangem a qualidade de código, padrões de codificação, vulnerabilidades de dependências, modelo relacional de banco de dados e concepção arquitetural.

Para a realização desta análise, gerou-se a tag *ctis-nota-tecnica-20200526* no repositório <https://git.prf/sistemas-nacionais/cggp-cga/siadi/> com referência branch master na data de 26/05/2020.

3 Apresentação do cenário atual

Esta sessão ira descrever a arquitetura, tecnologias, frameworks e dependências que compõe a base da aplicação.

O sistema DPRF Segurança foi construído para funcionar em ambiente WEB, utiliza tecnologia Java e está estruturada arquiteturalmente como uma aplicação monolítica (entende-se por este termo quando o sistema é composto por camadas de interface com usuário, camada de aplicação de regras negociais e camada de acesso a dados combinadas em uma única aplicação), utiliza o banco de dados *PostgreSQL*.

Sua arquitetura é composta por um único artefato que contém classes controladoras, classes de persistencia, classes para mapeamento ORM, classes utilitárias, classes para expor API's Rest, arquivos xhtml, css e javascript.

O diagrama a seguir representa o modelo de componentes ao qual a aplicação está construída.

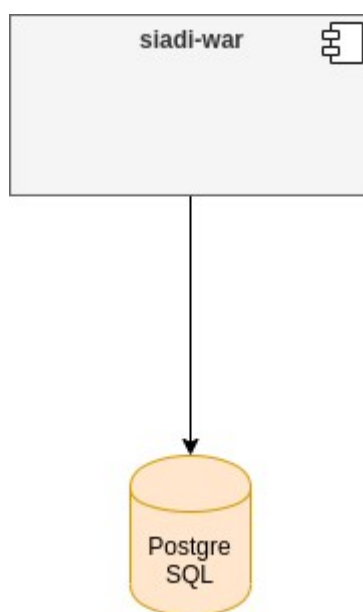


Figura 1: Diagrama de sequências



A aplicação utiliza o modelo MVC para a segregação de responsabilidades em camadas sendo que as requisições http são oriundas das páginas JSF. O diagrama a seguir representa os fluxos encontrados durante o processo de análise da aplicação, o diagrama representa também a falta de padronização comportamental da mesma.

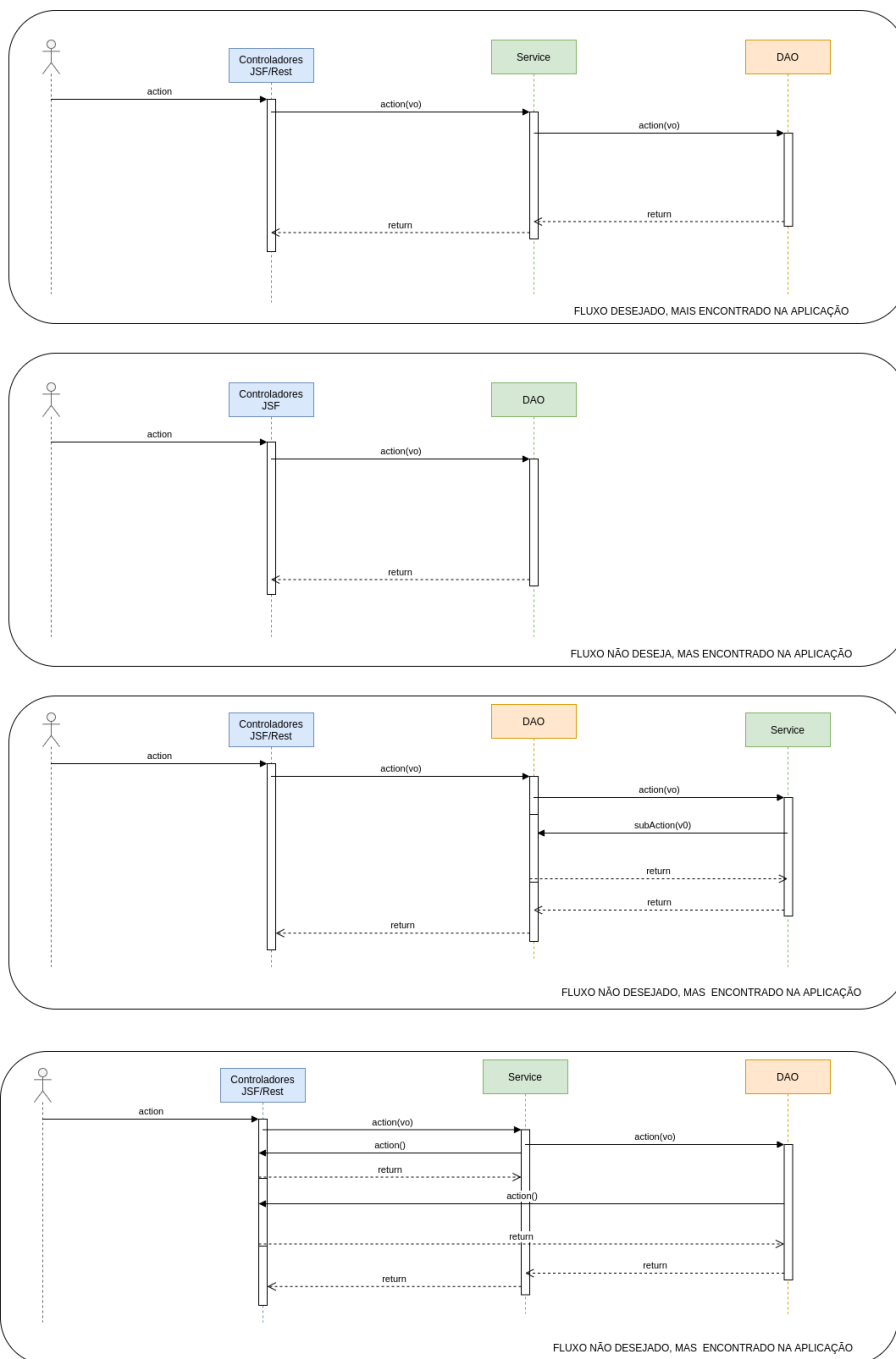


Figura 2: Diagrama de sequências



A solução utiliza um único schema com 52 tabelas.

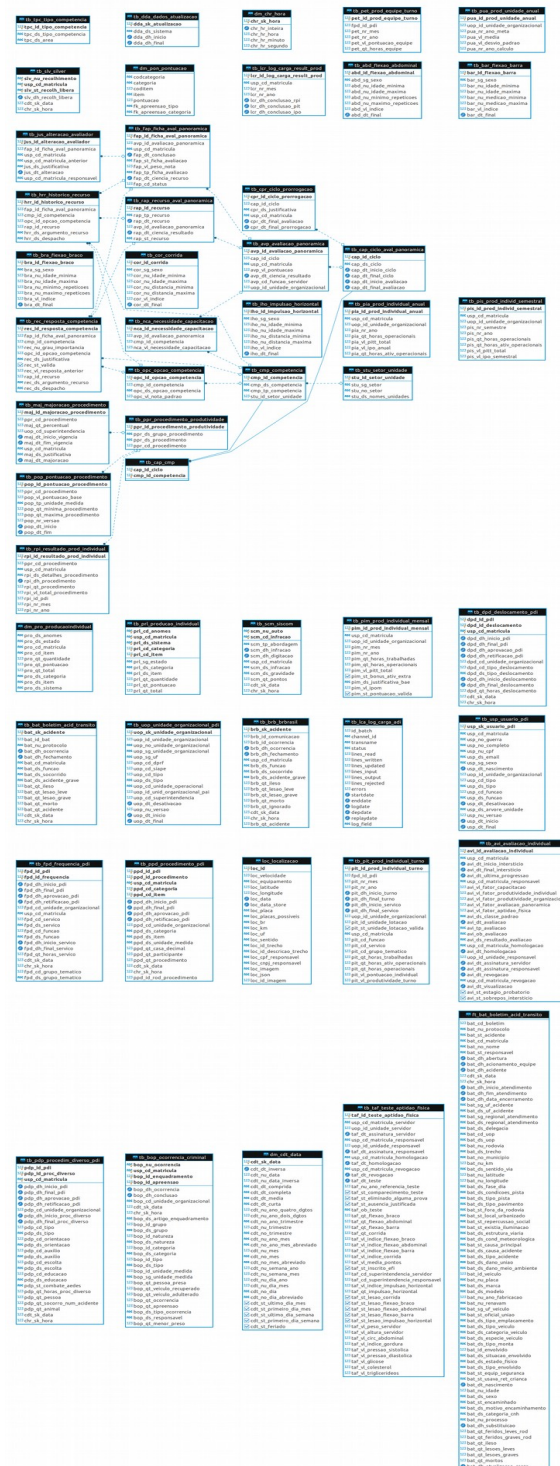


Figura 3: MER - banco
dbprodindividualD

3.1 Tecnologias utilizadas

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

Nome	Versão	Utilização	Observação
Java	1.8	Linguagem de programação.	
Hibernate	5.2.6	Framework ORM.	
Primefaces	6.2	Extensão de componentes JSF	
EJB	3.1.2	Container EJB para injeção de dependências.	
Wildfly	10.x	Servidor de aplicação JEE.	Utiliza container CDI e Servlet.
PostgreSQL		Banco de dados relacional	

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 SonarQube

Ferramenta utilizada para verificação de estática de código. Para esta análise não foram utilizadas as métricas de qualidade implantadas no SonarQube da DPRF, contudo foram utilizadas as regras padrões de análise da ferramenta.

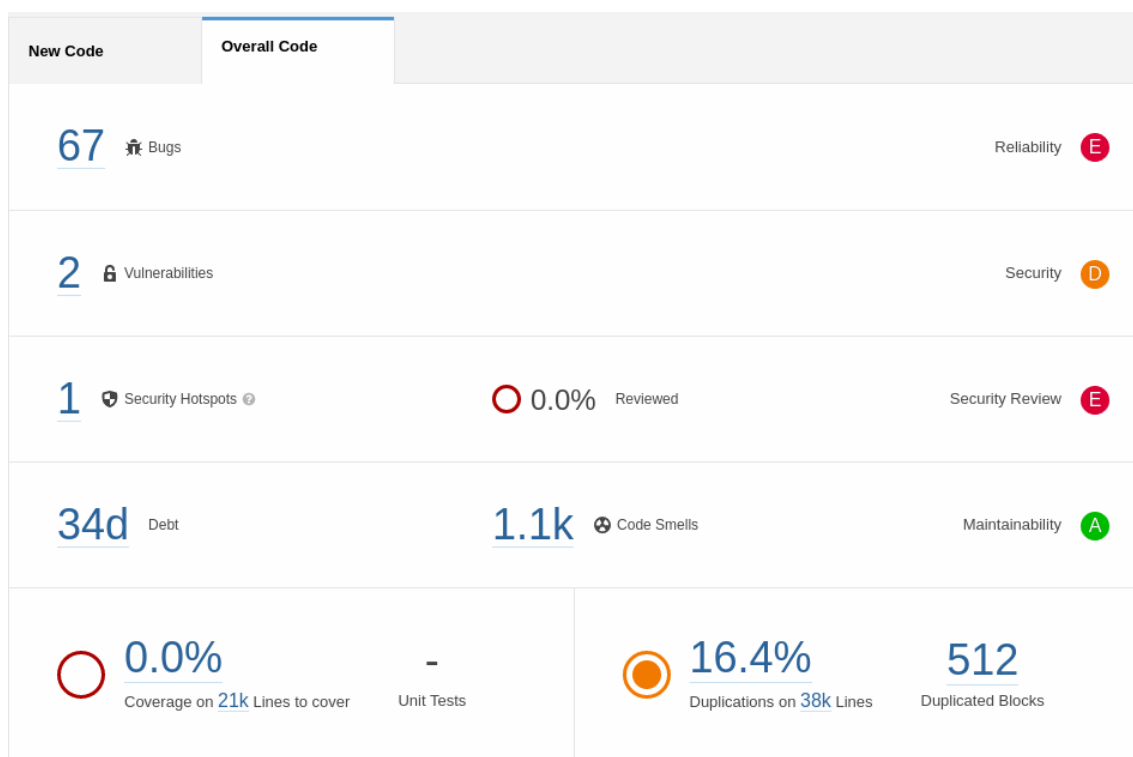


Figura 4: Sonarqube - análise estática de código

DPRF	DPRF Segurança - Nota técnica	
-------------	--------------------------------------	--

- 67 bugs;
- 2 vulnerabilidades de código;
- 35 violações de segurança;
- 1.100 violações de código ruim (complexidade cognitiva , complexidade ciclomática e débito técnico);
- 16,4% de duplicidade de código

4.2 OWASP Dependency Check

A utilização de bibliotecas de terceiros aumenta substancialmente a produtividade na construção de um software, contudo estas podem trazer consigo vulnerabilidades que afetam diretamente a segurança da aplicação. A ferramenta Dependency Check tem como propósito efetuar análise de vulnerabilidade de dependências utilizadas na construção deste projeto, a seguir temos as principais informações extraídas desta análise, a relação completa desta análise está disponível no Anexo I deste documento.

Dependency	Highest Severity	CVE Count	Confidence	Evidence Count
commons-beanutils-1.9.2.jar	HIGH	1	Highest	37
commons-collections-3.2.1.jar	CRITICAL	3	Highest	35
primefaces-6.2.jar	MEDIUM	1	Highest	28
hibernate-validator-5.2.4.Final.jar	HIGH	1	Highest	34
cdi-api-1.2.jar	MEDIUM	1	Low	36
javax.faces-api-2.2.jar	MEDIUM	1	Highest	43
shiro-core-1.2.5.jar	CRITICAL	2	Highest	32
httpclient-4.2.6.jar	MEDIUM	2	Highest	34
dom4j-1.6.1.jar	CRITICAL	2	Highest	25
itextpdf-5.5.9.jar	HIGH	1	High	31
poi-3.15.jar	HIGH	2	Highest	29
jquery.js	medium	3		3
primefaces-6.2.jar: jquery.js	MEDIUM	2		3

4.3 OWASP ZAP

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

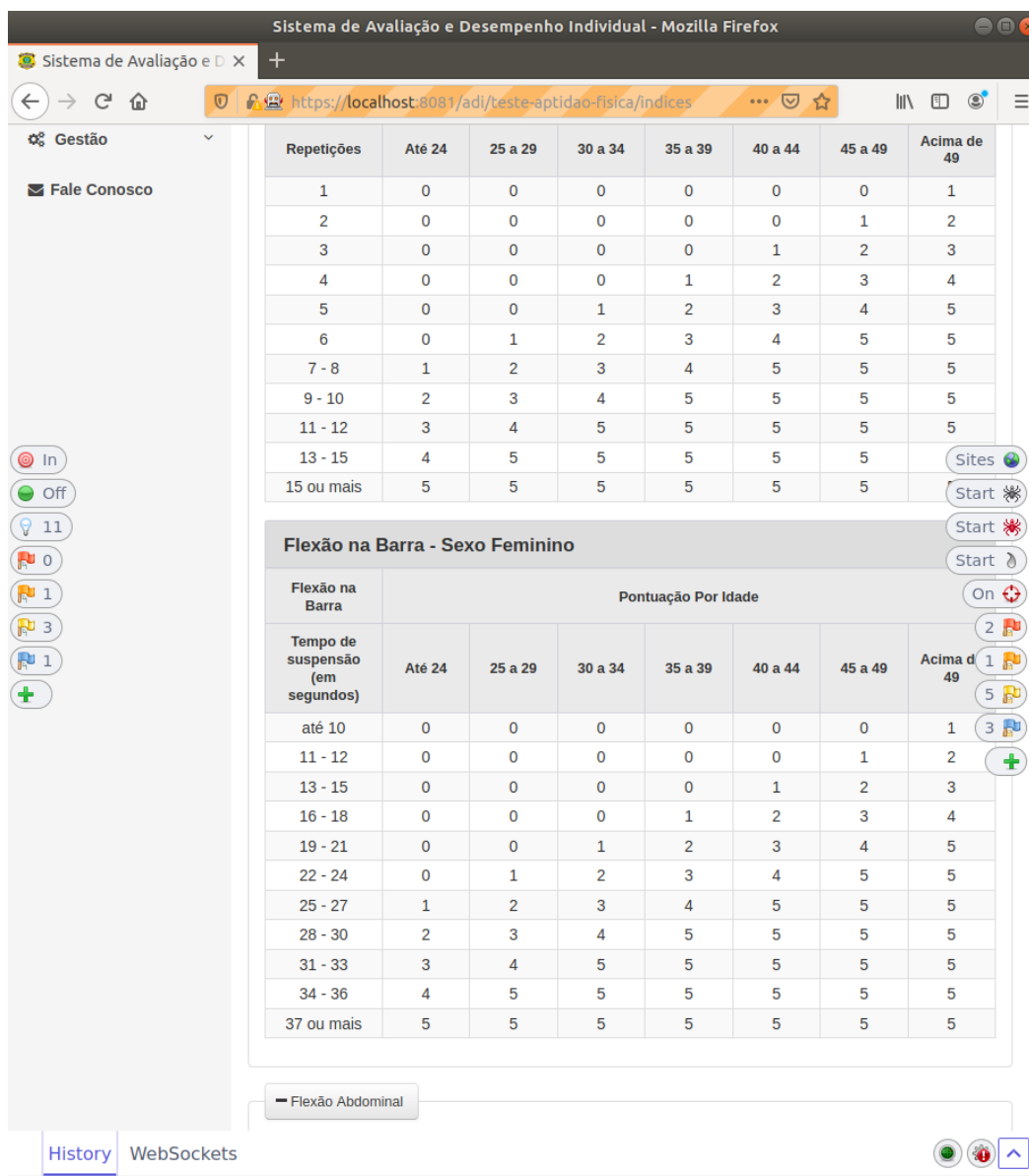


Figura 5: OWASPZAP - análise de intrusão

DPRF	DPRF Segurança - Nota técnica	
-------------	--------------------------------------	--

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

O relatório completo dos testes aplicados estão disponíveis no anexo I deste documento.

4.4 Estrutura do projeto

O projeto possui boa organização estrutural, sua segregação por pacotes é adequada e de fácil entendimento. Esta estrutura certamente facilita manutenções corretivas/evolutivas na ferramenta.

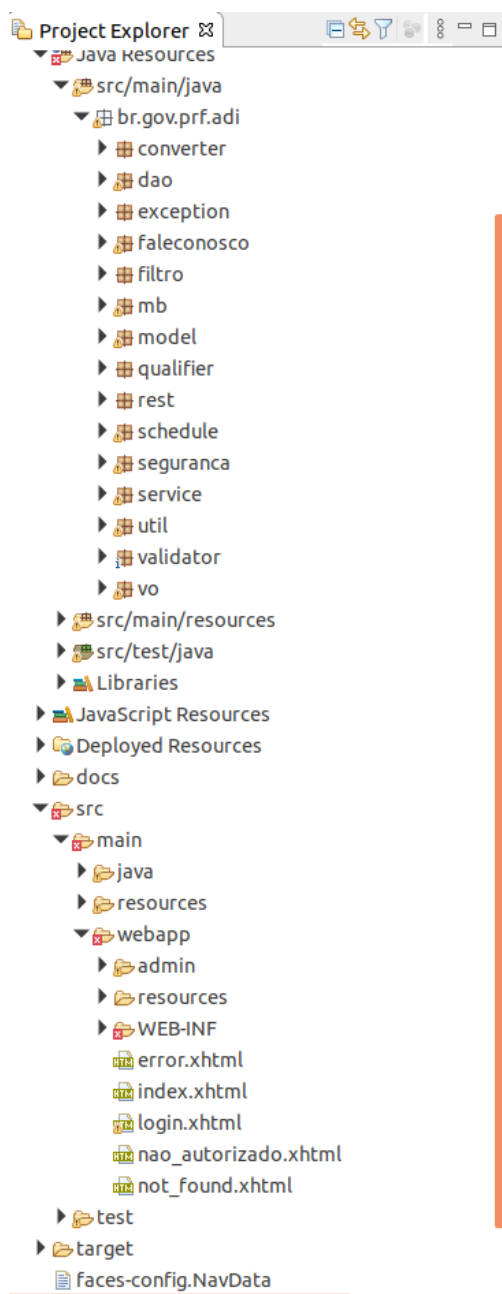


Figura 6: Estrutura do projeto



4.5 Manutenibilidade de código

Os relatórios apresentados pela ferramenta SonarQube demonstram uma série de vícios adotados durante o processo de construção do software e alinhado a estes vícios, a inexistência de cobertura de testes de unidade que trazem a dificuldade no processo de refactoring da aplicação, uma vez que não há condições de mensurar impactos durante o processo de manutenção corretiva/adaptativa.

A alta complexidade ciclométrica e a falta de artefatos de testes de unidade dificultam o processo de refactoring, a ilustração que seguem demonstram o cenário apontado (OBS: a característica apresentada é utilizada de forma recorrente em diversos momentos do código).

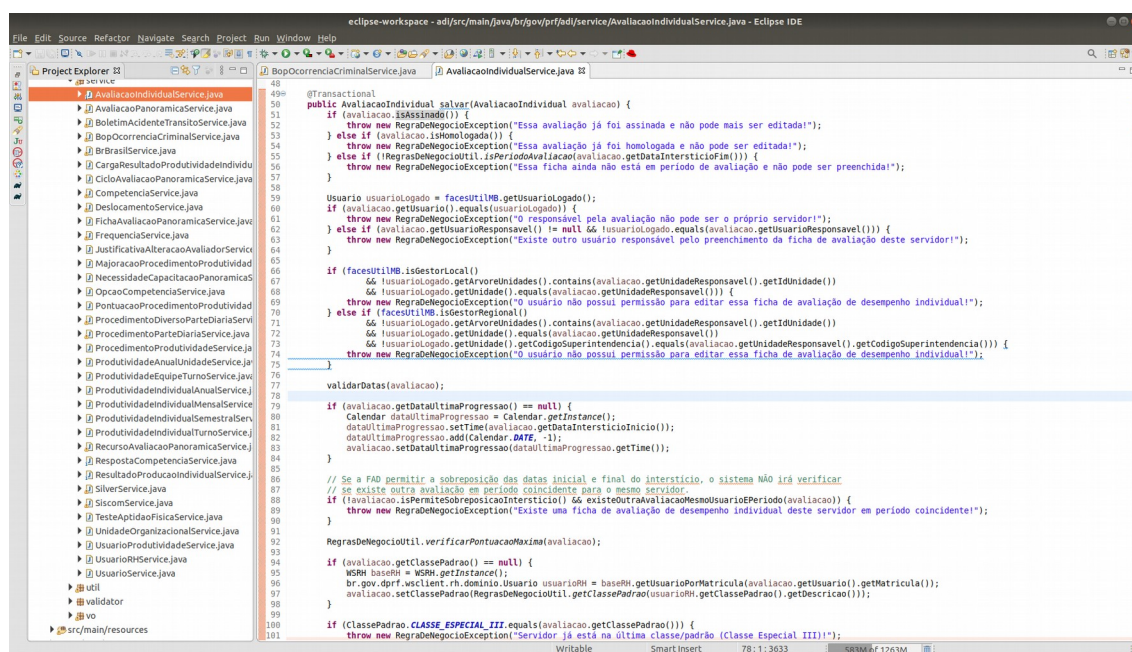


Figura 7: Complexidade ciclométrica

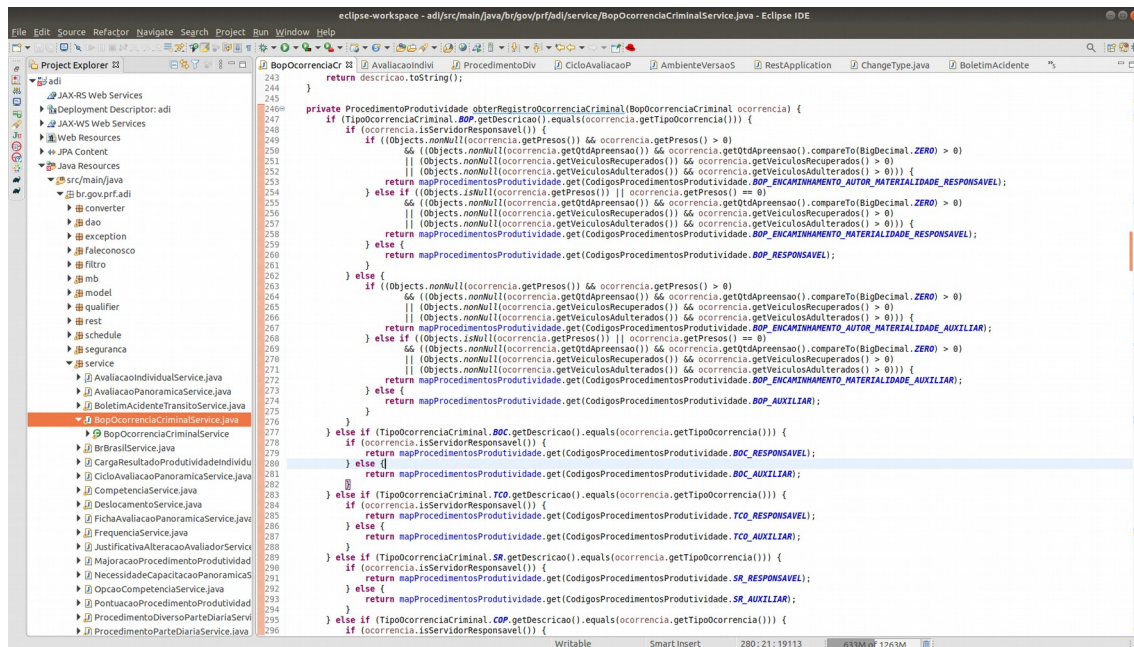


Figura 8: Complexidade ciclômática

Durante o processo de análise foi encontrado classes com grande volume de código e baixa coesão, uma vez que estas classes acabam extrapolando sua competência negocial.

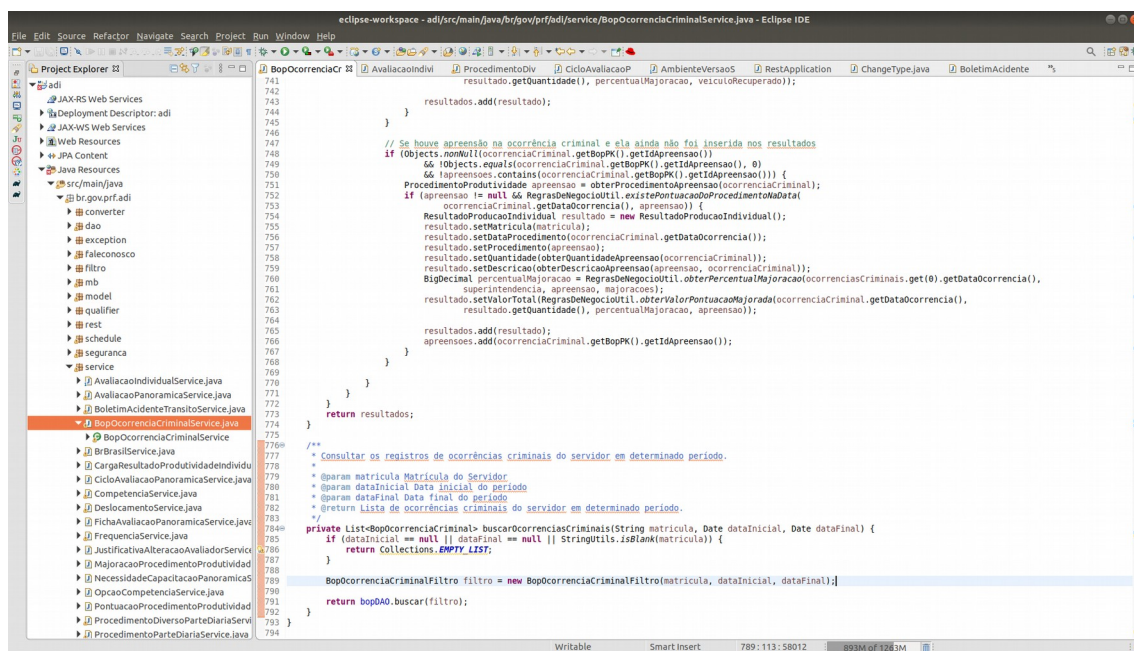


Figura 9: Classes grandes extrapolando sua competência negocial



Os furos arquiteturais são outro fator que prejudicam a manutenibilidade do código, uma vez que os fluxos apresentados nos diagramas de sequencias furam o preceito do padrão proposto ao modelo MVC.

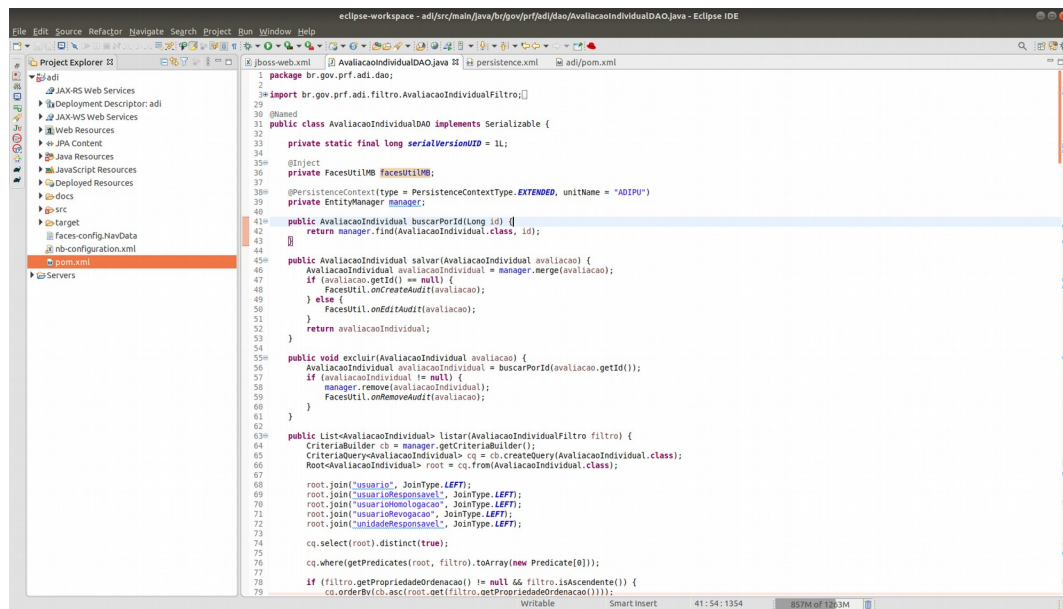


Figura 10: Camada de persistência acessando controladores

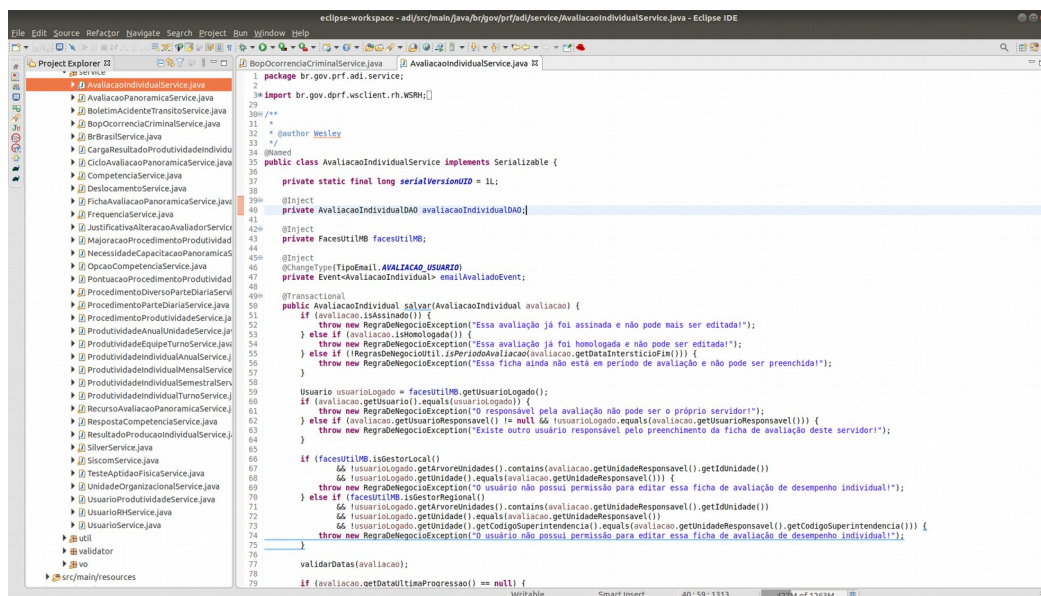


Figura 11: Controladores acessando camada de persistência



Outra característica encontrada durante o processo de análise de código foi a descentralização das validações de regras negociais. Uma vez que a mesma deveria estar concentrada na camada de serviço, estas validações são vistas nas classes controladores (que deveriam apenas controlar o ciclo de vida dos formulários) como também nas classes de persistência (ao qual deveria unicamente acessar o banco de dados).

Essa descentralização são fatores negativos para o entendimento negocial quanto para a manutenção do mesmo.

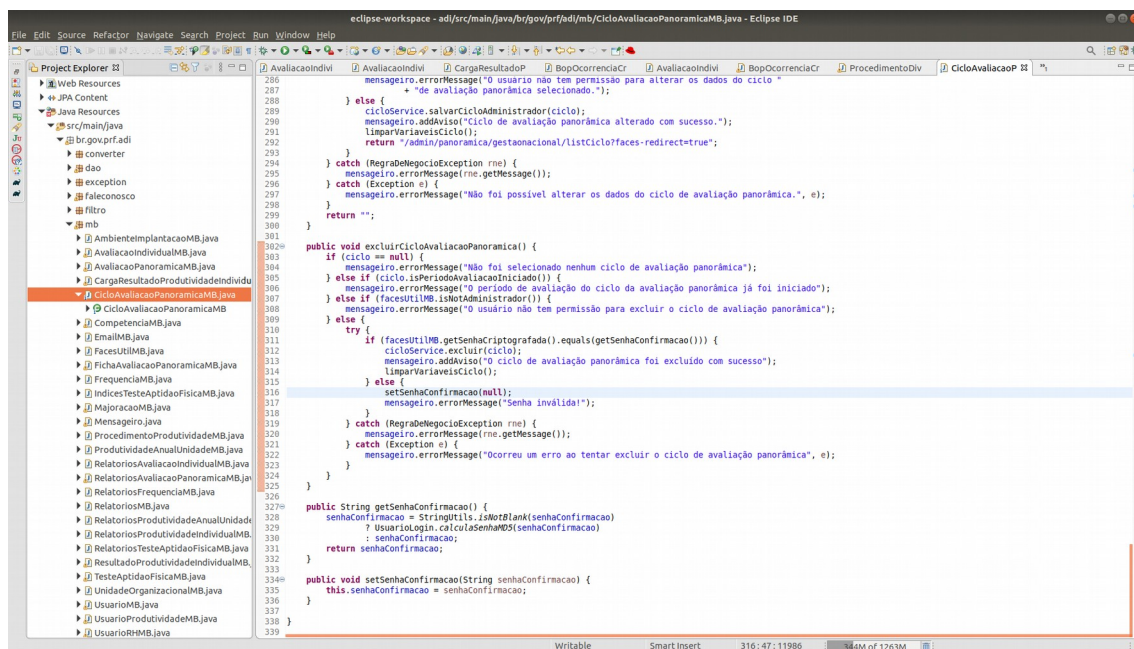
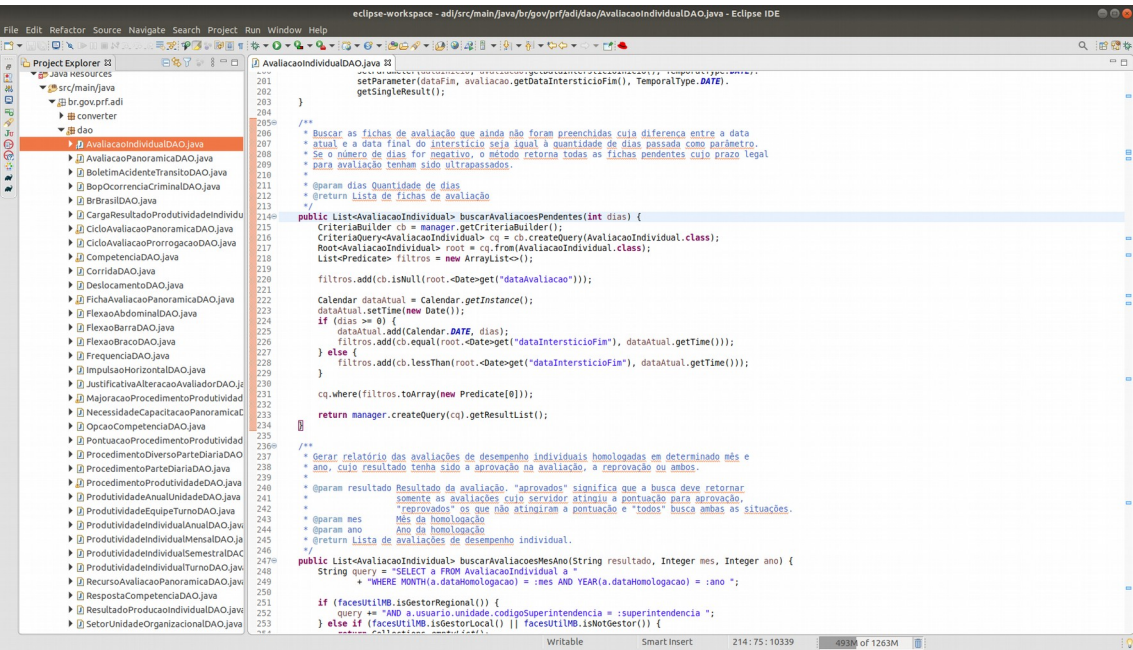


Figura 12: Controladores efetuando validações negociais.



```
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000
```

Figura 13: Classes de persistência validando condições negociais para tomada de decisão

4.6 Confiabilidade

Há controle de transação a nível de aplicação, esta é uma boa prática sendo que a mesma está sendo aplicada na camada de serviço. Esta prática garante as propriedades ACID do banco de dados, garante também consistência da informação uma vez que vários dados podem ser modificados em uma única transação.

A manutenção da consistência de dados é algo fortemente desejado, contudo esta não garante toda a confiabilidade da solução. A quantidade elevada de bugs, vulnerabilidades no código, bibliotecas de terceiros encontradas e as vulnerabilidades encontradas durante o processo de análise de intrusão demonstradas nos relatórios apresentados trazem riscos a confiabilidade da ferramenta.

4.7 Performance e estabilidade

Não foi analisado o funcionamento da aplicação para avaliar demais requisitos não funcionais, recomenda-se a utilização de ferramentas de APM para mensurar performance e recursos de máquina utilizados.

A arquitetura monolítica citada no tópico 3 deste documento prejudica a escalabilidade da ferramenta, os recursos empreendidos para a escalabilidade vertical (aumento de recursos de processamento, disco, memória e demais) são limitados e onerosos.

A escalabilidade vertical do monólito é possível levando em consideração o aumento de nós no cluster, contudo esta escalabilidade é prejudicada tendo em vista que temos que escalar a aplicação como um todo, necessitando assim da mesma quantidade de recursos empreendidas nos demais nós existentes. Nesta arquitetura não há a possibilidade de escalar somente as funcionalidades/módulos que mais são demandados.

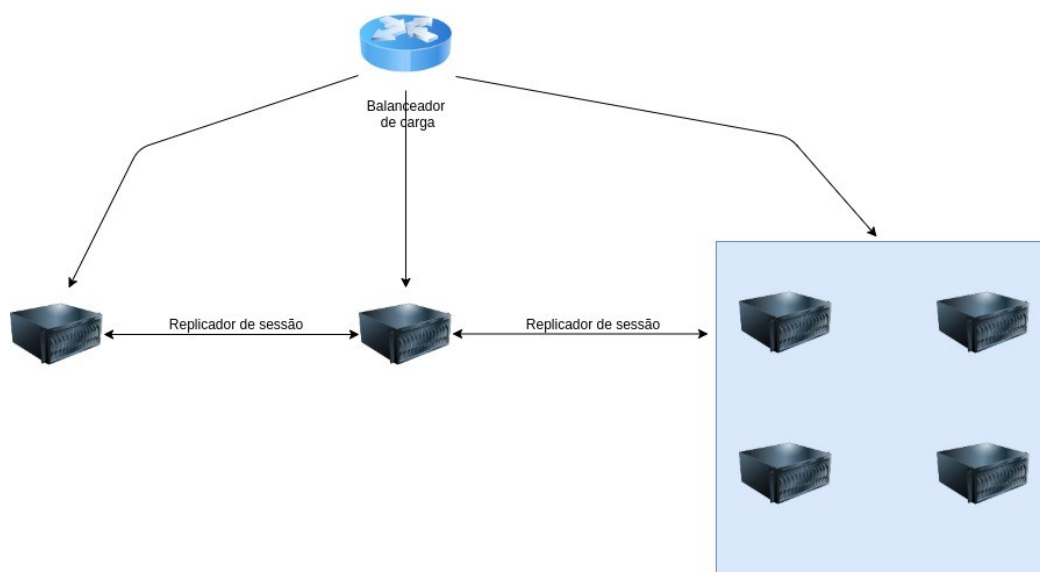


Figura 14: Escalabilidade do monólito

5 Recomendações

É altamente recomendado que seja efetuado refactoring de código dos bugs e vulnerabilidades de código apontadas pelo SonarQube , estas atividades certamente trarão maior confiabilidade a ferramenta e estabilidade em seu uso. Para os demais itens apontados pela ferramenta SonarQube durante o processo de análise de código são altamente desejáveis, contudo este processo de ajuste de código é moroso e trás consigo risco em potencial e está diretamente aliado a falta de cobertura de testes de unidade.

Ajustar as dependências que trazem maior risco para a aplicação é altamente recomendável, contudo este trabalho deve ser feito de forma analítica e cautelosa afim de não prejudicar a estabilidade da ferramenta. Sugere-se a associação dos relatórios de análise de dependências com os relatórios de análise de intrusão para que sejam analisados as principais vulnerabilidades da aplicação e associá-las as dependências que oferecem tais riscos para os devidos ajustes. Esta recomendação esta embasada na interseção de resultados das ferramentas utilizadas e na otimização e na assertividade do trabalho de refactoring. Vale ressaltar a necessidade de correção das vulnerabilidades de XSS e SQL Injection encontradas durante o processo de análise de intrusão.

Recomenda-se a implantação de ferramentas de APM para que sejam criadas métricas e alarmes que auxiliem na continuidade do serviço em ambiente produtivo(monitoramento de processamento e memória por exemplo), tendo em vista que este tipo de ferramenta fornece mecanismos para determinarmos o comportamento da solução (auxiliam no refactoring de código) e também subsidia para o correto dimensionamento da infraestrutura.

Recomenda-se o desacoplamento das atividades executadas em batch (Quartz) do cor da aplicação, uma vez que esta prática

DPRF	DPRF Segurança - Nota técnica	
-------------	--------------------------------------	--

promove a concorrência de recursos da aplicação principal e dificulta a escalabilidade horizontal. Vale ressaltar que ao segregar os serviços batch do core da aplicação, recomenda-se segregar os demais componentes (classes negociais, serviço, persistência e etc) para que se promova o reuso dos componentes.

Recomenda-se também o ajuste dos fluxos de execução da aplicação, uma vez que não um comportamento uniforme, temos classes de serviço acessando controladores e classes de persistência acessando classes de serviço. Esta prática não promove o princípio da abstração da orientação a objetos aplicado ao modelo MVC.

Para fins de organização e padronização, recomenda-se que seja mantido de forma permanente 3 branches no repositório GIT e que estas representem especificamente os ambientes ao qual estão implantadas, sendo elas master, homologação e desenvolvimento. Recomenda-se que ao mergear uma nova branch a master, que esta seja removida e uma nova tag seja gerada.