



**CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA
CELSO SUCKOW DA FONSECA
UNIDADE DE ENSINO DESCENTRALIZADA DE NOVA FRIBURGO/RJ**

TIELLE DA SILVA ALEXANDRE
tiellesa@gmail.com

BLACKURLLIGHT LIST

**Nova Friburgo
2015**



**CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA
CELSO SUCKOW DA FONSECA
UNIDADE DE ENSINO DESCENTRALIZADA DE NOVA FRIBURGO/RJ**

TIELLE DA SILVA ALEXANDRE
tiellesa@gmail.com

BLACKURLLIGHT LIST

Trabalho de conclusão de curso apresentado ao
CEFET Nova Friburgo como requisito parcial para
a conclusão do Curso Técnico de Informática

**Nova Friburgo
2015**



**CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA
CELSO SUCKOW DA FONSECA
UNIDADE DE ENSINO DESCENTRALIZADA DE NOVA FRIBURGO/RJ**

Curso: Técnico em Informática

Ano: 2015

Aluno 1: Tielle da Silva Alexandre

Título do TCC: BlackURLLight List

Orientador: Nilson Mori Lazzarin

Nota:

Recomendações:

(Docente Orientador)

Nova Friburgo, ____ de _____ de _____

Agradecimentos

As (...)

BlackURLLight List

Tielle da Silva Alexandre

Resumo. Uma lista de catalogação é usada na configuração de regras de acesso em um servidor *Proxy* a fim de intermediar o acesso a conteúdos acessados por usuários de uma rede local. A *URLBlackList* é uma das listas de catalogação disponível para o processo de controle de conteúdo, entretanto, esta possui domínios não resolvíveis e anomalias que precisam ser reparadas para otimizar o processo de controle de conteúdo. Sendo assim, esse projeto tem como objetivo reduzir o tempo e os recursos computacionais utilizados por um servidor *Proxy* através de um processo de refinamento da *URLBlackList*. Como solução, o projeto propõe desenvolver um sistema *web*, utilizando o *Java Enterprise Edition*, capaz de segmentar os domínios pertencentes à *URLBlackList* em dois grupos: os domínios resolvíveis e os não resolvíveis, além de expurgar qualquer anomalia encontrada. Após o processo de refinamento, o sistema possibilitará a geração de uma lista de catalogação enxuta composta somente por domínios resolvíveis que efetivamente devem ser utilizados no processo de controle de conteúdo. O projeto propõe ainda, uma análise comparativa e qualitativa entre a lista gerada pela *BlackURLLightList* e a lista da *URLBlackList*.

Palavras-chave: Redes de Computadores, *URLBlackList*, desenvolvimento web.

Responsável por publicações:

<Inserir Nome da Responsável Aqui>

Biblioteca do CEFET UnED Nova Friburgo
Av. Governador Roberto Silveira, 1900 – Prado
28.635-000 Nova Friburgo RJ Brasil
Tel. +55 22 2527-1727
E-mail: biblionf@gmail.com

Tabelas

Tabela 1. Resumo dos Resultados Obtidos.....	26
Tabela 2. CDU1 - Cadastrar Domínio.....	31
Tabela 3. CDU2 - Buscar Domínio.....	32
Tabela 4. CDU3 - Alterar Domínio.....	33
Tabela 5. CDU4 - Excluir Domínio.....	34
Tabela 6. CDU5 - Cadastrar Administrador.....	35
Tabela 7. CDU6 - Buscar Administrador.....	36
Tabela 8. CDU7 - Alterar Administrador.....	37
Tabela 9. CDU8 - Alterar Grau de Perversidade.....	38
Tabela 10. CDU9 - Listar Categoria.....	39
Tabela 11. CDU10 - Listar Reclassificação.....	40
Tabela 12. CDU11 - Excluir Reclassificação.....	41
Tabela 13. CDU12 - Reclassificar Categoria.....	42
Tabela 14. CDU13 - Gerar BlackURLLightList - Inativa.....	43
Tabela 15. CDU14 – Gerar BlackURLLightList No Formato BlackList.....	44
Tabela 16. CDU15 – Gerar BlackURLLightList Reclassificada.....	45
Tabela 17. CDU16 – Analisar Arquivo da URLBlackList.....	48
Tabela 18. CDU17 – Analisar Banco de Dados.....	50
Tabela 19. CDU18 – Baixar URLBlackList.....	51
Tabela 20. CDU19 – Verificar Versão URLblackList.....	52
Tabela 21. CDU20 – Efetuar Login.....	53
Tabela 22. CDU21 – Efetuar Logoff.....	54
Tabela 23. CDU22 – Download BlackURLLightList.....	55

Figuras

Figura 1. A hierarquia do DNS para o domínio <code>noticiais.cefet-rj.br</code>	16
Figura 2. O conteúdo da categoria <code>adult</code>	17
Figura 3. O <code>dig</code> para o domínio <code>cefet-rj.br</code>	18
Figura 4. O <code>dig</code> para um domínio que não resolve.....	19
Figura 5. A metodologia da <code>BlackURLLightList</code>	21
Figura 6. A arquitetura Cliente-servidor.....	24
Figura 7. O diagrama de caso uso da <code>BlackURLLightList</code>	30
Figura 8. Diagrama de Classe Conceitual.....	56
Figura 9. Diagrama de Classe Coleções.....	57
Figura 10. Diagrama de Classe Parcial - Analisar Arquivo <code>URLBLackList</code>	58
Figura 11. Diagrama de Classe Parcial - Analisar Banco de Dados.....	59
Figura 12. Diagrama de Classe Parcial - Gerar <code>BlackURLLightList</code> – Ativa.....	60
Figura 13. Diagrama de Classe Parcial - Gerar <code>BlackURLLightList</code> – Inativa.....	61
Figura 14. Diagrama de Sequência - Analisar Banco de Dados.....	62
Figura 15. Diagrama de Sequência - Gerar <code>BlackURLLightList</code> – No Formato <code>BlackList</code>	63
Figura 16. Diagrama de Sequência - Gerar <code>BlackURLLightList</code> – Inativa.....	64
Figura 17. Diagrama de Atividade - Analisar Banco de Dados.....	65
Figura 18. Diagrama de Atividade - Analisar Arquivo <code>URLBLackList</code>	66
Figura 19. <i>O DER relativo a BlackURLLightList</i>	67
Figura 20. <i>Arquivo JAR</i>	68
Figura 21. Diretório para instalação <code>DIG</code>	69
Figura 22. Mapa de navegação.....	70
Figura 23. Tela de Gerenciamento do Grau de Perversidade.....	70
Figura 24. Tela de Reclassificação de Categorias.....	71
Figura 25. Tela Analisar Arquivo <code>URLBlackList</code>	71
Figura 26. Tela Analisar Banco de Dados.....	72
Figura 27. Tela Gerar <code>BlackURLLightList</code> - Ativa.....	73

Anexos

Anexo I – Categorias *URLBlackList*.

Anexo II – Tabelas de Resultado Obtido por Categoria.

Anexo III - Tabela de Grau de Perversidade

Anexo IV - Modelo Lógico e Modelo Físico do Banco de Dados

Sumário

1 Introdução

1.1	Problema	12
1.2	Objetivo.....	13
1.3	Estrutura do Trabalho.....	14

2 Revisão Bibliográfica 16

2.1	Domain Name System (DNS).....	16
2.2	URLBlackList	17
2.3	DIG.....	18

3 BlackURLLightList 20

3.1	A Metodologia	20
3.1.1	Processo de Refinamento	21
3.1.2	Processo de Análise de Redundância	22
3.1.3	Processo de Reclassificação de Categorias	23
3.2	Implementação da BlackURLLightList	24

4 Análise dos Experimentos 26

4.1	Análise.....	26
-----	--------------	----

5 Documentação do Sistema..... 28

5.1	Mini-Mundo	28
5.2	Diagrama de Casos de Uso.....	29
5.3	Descrição de Casos de Uso	30
5.3.1	Caso de Uso 1 – Cadastrar Domínio	31
5.3.2	Caso de Uso 2 – Buscar Domínio	32
5.3.3	Caso de Uso 3 – Alterar Domínio	33
5.3.4	Caso de Uso 4 – Excluir Domínio.....	34
5.3.5	Caso de Uso 5 – Cadastrar Administrador	35
5.3.6	Caso de Uso 6 – Buscar Administrador	36
5.3.7	Caso de Uso 7 – Alterar Administrador	37
5.3.8	Caso de Uso 8 – Alterar Grau de Perversidade	38
5.3.9	Caso de Uso 9 – Listar Categoria.....	39

5.3.10	Caso de Uso 10 – Listar Reclassificação.....	40
5.3.11	Caso de Uso 11 – Excluir Reclassificação	41
5.3.12	Caso de Uso 12 – Reclassificar Categoria.....	42
5.3.13	Caso de Uso 13 – Gerar BlackURLLightList - Inativa	43
5.3.14	Caso de Uso 14 – Gerar BlackURLLightList No Formato BlackList.....	44
5.3.15	Caso de Uso 15 – Gerar BlackURLLightList Reclassificada	45
5.3.16	Caso de Uso 16 – Analisar Arquivo da URLBlackList.....	46
5.3.17	Caso de Uso 17 – Analisar Banco de Dados	49
5.3.18	Caso de Uso 18 – Baixar URLBlackList.....	51
5.3.19	Caso de Uso 19 – Verificação URLBlackList.....	52
5.3.20	Caso de Uso 20 – Efetuar Login	53
5.3.21	Caso de Uso 21 – Efetuar Logoff.....	54
5.3.22	<i>Caso de Uso</i> 22 – Download BlackURLLightList.....	55
5.4	Digramas de Classes.....	56
5.4.1	Diagrama de Classe Conceitual.....	56
5.4.2	Diagrama de Classe Coleções	57
5.4.3	Diagrama de Classe Parcial – Analisar Arquivo URLBlackList.....	58
5.4.4	Diagrama de Classe Parcial – Analisar Banco de Dados	59
5.4.5	Diagrama de Classe Parcial – Gerar BlackURLLightList - Ativa.....	60
5.4.6	Diagrama de Classe Parcial – Gerar BlackURLLightList – Inativa.....	61
5.5	Diagramas de Sequência	62
5.5.1	Diagrama de Sequencia – Analisar Banco de Dados	62
5.5.2	Diagrama de Sequencia – Gerar BlackURLLightList (Formato BlackList)	63
5.5.3	Diagrama de Sequencia – Gerar BlackURLLightList – Inativa.....	64
5.6	Diagramas de Atividade	65
5.6.1	Diagrama de Atividade – Analisar Banco de Dados	65
5.6.1	Diagrama de Atividade – Analisar Arquivo URLBlackList	66
5.7	Projeto de Banco de Dados	67
6	Manual do Sistema.....	68
6.1	Manual de Instalação.....	68
6.1.1	Sistema Operacional <i>Windows</i>	69
6.2	Manual de Utilização	69
7	Conclusão.....	74
8	Referências Bibliográficas.....	86

1 Introdução

Segundo (IBOPE, 2013), no terceiro trimestre de 2012, 94,2 milhões de brasileiros possuem acesso à internet. Esse número considera o acesso à internet realizado em qualquer ambiente e a pesquisa ainda pondera que os ambientes com maior totalidade de acesso são os ambientes de trabalho e domicílio e que a idade desses internautas compreende a faixa etária que vai dos 2 anos de idade em diante. Os números apontados apenas comprovam que a internet está cada vez mais acessível e que se consolida como uma das principais fontes de informação para a população.

A internet proporciona o acesso a diversos tipos de conteúdo e que a informação circule em tempo real. Esse dinamismo virtual corrobora com a era da globalização que vivenciamos, onde a interligação de informações e a interatividade entre as pessoas acontecem como se não houvesse fronteiras. Esse fato é evidenciado pelos diversos sites de relacionamentos virtuais que se firmaram como meios de comunicação contemporâneos. Os internautas utilizam os *sites* de relacionamento para conhecer e manter o contato com pessoas que podem estar a milhas de distância, além de expressar opiniões, ideias e até mesmo promover ou não protestos (COUTINHO, 2012).

Ora por entretenimento, ora por busca de conhecimento, a internet está presente na vida das pessoas e diante de um mundo virtual sem fronteiras, algumas questões pertinentes ao livre acesso à internet são levantadas. Por exemplo, em determinados ambientes como instituições de ensino, empresas e bibliotecas, as políticas de acesso à internet são adotadas para impedir que os usuários tenham acesso a sites de relacionamentos, sites com conteúdo de vídeos, games ou pornografia. Dependendo do ambiente, os conteúdos acessados pelos usuários são considerados inadequados de acordo com a cultura organizacional.

Nesse contexto, as políticas de acesso à internet estabelecem regras ou restrições de acesso que são fundamentais para assegurar que algumas condutas sejam respeitadas pelo usuário. Essas regras de acesso são configuradas pelos administradores de redes que utilizam a combinação de um servidor *Proxy* e de arquivos que contenham uma lista catalogada com os domínios para criar um filtro de acesso, impedindo que determinados conteúdos, considerados indevidos pelas políticas de acesso de uma organização, sejam acessados pelo usuário.

Segundo Morimoto (2009), um servidor *Proxy* analisa todas as requisições recebidas, separando o que pode e o que não pode trafegar pela rede. Trata-se de um intermediador entre computadores de uma rede local e a Internet que monitora todas as requisições envolvidas. O processo de filtragem de conteúdo por meio de um servidor *Proxy* ocorre através da comparação das requisições do cliente com uma lista de *Uniform Resource Locator* (URLs) ou domínios autorizados (lista branca) ou com uma lista de URL ou domínios não autorizados (lista negra) para liberar ou não o acesso à página solicitada.

O projeto *URLBlackList* fornece uma catalogação através de um arquivo compactado, composto por um conjunto de listas de URL, domínios e expressões subdivididas em, aproximadamente, 100 categorias. Esse conjunto de listas é utilizado por um servidor *Proxy* para realizar o controle de acesso à internet (URLBLACKLIST, 2015). A tabela *Categorias URLBlackList* no Anexo I contém uma listagem com todas as categorias existentes, atualmente, na lista da *URLBlackList*.

1.1 Problema

O catálogo de *sites* utilizado pelo administrador de redes é o fator estratégico de um processo de controle de conteúdo para que este funcione de maneira eficaz, proporcionando que as políticas de acesso à rede sejam respeitadas. Atualmente, o catálogo mais adotado é o da *URLBlackList*. Apesar disso, a catalogação disponibilizada pela *URLBlackList* possui alguns percalços que impossibilitam que o controle de acesso à sites seja realizado com um maior desempenho.

Quando um servidor *Proxy* recebe uma requisição de uma página, inicia-se um processo de comparação entre a requisição e todas as linhas de domínio presentes no arquivo da *URLBlackList*. Cada linha é verificada individualmente. Depois de percorrer toda a lista, o servidor *Proxy* autoriza ou não o acesso à página solicitada pelo cliente. Entretanto, a *URLBlackList* apresenta diversos *sites* catalogados que estão inativos e que, conseqüentemente, por constarem na lista, consomem processamento desnecessariamente. Como não há um mecanismo de atualização constante dessas listas com a exclusão dos *sites* inativos, os servidores até mesmo os mais robustos comprometem o seu desempenho percorrendo listas com conteúdos não íntegros.

Outro fator pertinente quando se refere à *URLBlackList* é a sua origem norte-americana cujas categorias dispostas sofrem certas distorções de entendimento quando traduzidas para nosso idioma. A categoria *guns* faz referência às armas de pequeno porte que são comercializadas livremente, já a categoria *weapons* contempla artefatos de guerra, cuja portabilidade não é permitida. No Brasil, não existe essa distinção e qualquer porte de arma deve passar por um processo de legalização. Sendo assim, esse é um dos casos em que as categorias poderiam ser unidas se utilizadas em um contexto brasileiro, pois não é coerente que existam duas categorias com significados idênticos.

Na *URLBlackList*, um domínio pode ser encontrado em mais de uma categoria, ocasionando uma redundância de verificação no servidor *Proxy*, pois um mesmo domínio pode ser verificado mais de uma vez. Por exemplo, quando um Administrador de Redes for estabelecer um bloqueio de acesso a conteúdos pornográficos em uma determinada rede local, provavelmente, deverá incluir em suas regras de bloqueio as categorias *Adult*, *Sexuality* e *Porn*, entretanto, vários domínios existem em concomitância nestas categorias, como é o caso do domínio *sexwork.com*. Dessa forma, um servidor *Proxy* desperdiça recursos computacionais analisando por várias vezes o mesmo domínio.

Analisando as listas de domínio das categorias da *URLBlackList*, é possível observar que existem IPs dentro dessas listas, o que revela uma situação inesperada, já que uma lista de domínios, logicamente, deveria possuir apenas domínios. Outro fato que pode ser verificado é a existência de domínios que possuem certas anomalias de formato, como por exemplo, os domínios *googlex.com* e *relato-sexo.com* que possuem dois pontos consecutivos. Esses domínios ocasionam falhas de resolução por serem tratados como domínios inválidos.

Diante dos problemas apresentados, existe a necessidade de se ter disponível uma lista catalogada enxuta apenas com domínios resolvíveis para que não ocorram desperdícios computacionais quando um servidor *Proxy* intermediar os acessos a páginas *web* de uma rede local. Além disso, é necessário que uma reclassificação das categorias da *URLBlackList* seja promovida a fim de proporcionar uma melhor adequação ao contexto brasileiro.

1.2 Objetivo

A ferramenta *BlackURLLightlist* utilizará como *input* de um processo de refinamento os registros de domínio da *URLBlackList* a fim de gerar uma lista enxuta somente com domínios resolvíveis e não redundantes, livre de qualquer anomalia de resolução e de IP. Além disso, a ferramenta possibilitará a geração de outra lista somente com os domínios não resolvíveis encontrados no processo de refinamento da *URLBlackList*. Essa lista terá como objetivo colaborar com o projeto de catalogação da *URLBlackList*, pois fornecerá a mesma um arquivo com os domínios que poderão ser retirados da lista. É importante ressaltar que essa ferramenta não possuirá nenhuma integração direta com a *URLBlackList* e que a lista gerada de domínios não resolvíveis será repassada à mesma por meio de um *e-mail*, uma vez que esse é o único meio de contato/atualização disponibilizado pelo projeto.

A ferramenta possibilitará ao Administrador de Redes realizar a reclassificação das categorias da *URLBlackList* a fim de adequá-las ao contexto brasileiro. Sendo assim, o

Administrador de Redes poderá unificar as categorias consideradas sinônimas em uma única categoria. Isso proporcionará à geração de uma lista cujas categorias não estejam atreladas a linguagem americana. Além disso, a ferramenta desenvolvida otimizará o desempenho do servidor *Proxy* através do tratamento de redundâncias de domínios encontrados em mais de uma categoria na *URLBlackList*. O domínio *facebook.com*, por exemplo, está presente nas categorias *socialnetworking* e *social_networks*, sendo assim, em um processo de filtragem o mesmo domínio passa por duas vezes nesse processo. Através de um tratamento de redundância, esse domínio estará presente em apenas uma categoria ocasionando a racionalização de recursos computacionais envolvidos no processo de filtragem de um servidor *Proxy*. A fim de disponibilizar a lista gerada pela ferramenta para que outros usuários tenham acesso e a utilizem em seus processos de controle de conteúdo, esse projeto deverá ter um link para *download*.

A ferramenta *BlackURLLightList* terá ainda uma área administrativa que será disponibilizada para o gerenciamento de todo o processo de refinamento, bem como a geração das listas da *BlackURLLightList*. Nessa área, também será possível realizar as seguintes funcionalidades:

- O gerenciamento de domínios;
- A reclassificação das categorias;
- O controle dos parâmetros necessários para que o tratamento de redundância seja realizado de acordo com os critérios estabelecidos pelo Administrador de Redes;
- A verificação se existe uma nova versão da lista da *URLBlackList* disponibilizada para *download*.

Após o *download* do arquivo da *URLBlackList*, o mesmo deve ser descompactado para que o processo de refinamento possa ser iniciado. A ferramenta iniciará a leitura do arquivo de domínio pertencente a uma categoria e um sistema de nome de Domínio (*Domain Name System* - DNS), que é um protocolo responsável pelo mapeamento do endereço IP utilizado por um domínio. Em seguida, começa a verificar a existência de um IP que esteja associado ao domínio que está sendo percorrido pela leitura do arquivo. (MORIMOTO, 2009). O processo de resolução de domínio acontecerá da seguinte forma:

1. Uma consulta será realizada em um servidor DNS raiz à procura do IP associado aquele domínio;
2. Caso o servidor DNS não resolva, o domínio consultado não está associado a um número de IP, sendo assim, é identificado que aquele domínio está inativo ou indisponível para acesso na *web*;
3. Caso o servidor DNS resolva, o domínio consultado possui um endereço IP associado.

A partir desse *feedback* do servidor DNS, um domínio poderá receber um *status* de resolução (resolvível ou não resolvível). Após o processo de resolução, o domínio será cadastrado no banco de dados com o *status* de resolução. Esse processo de refinamento se repete para cada arquivo de domínio da *URLBlackList* associado a uma categoria. Além disso, a ferramenta deverá oferecer a possibilidade de atualização do *status* dos domínios já cadastrados.

1.3 Estrutura do Trabalho

Este trabalho está estruturado da seguinte forma: no capítulo 2 será apresentada a revisão bibliográfica que envolverá os conceitos básicos para entendimento do desenvolvimento do projeto: o *Domain Name System* (DNS); a *URLBlackList*; e o utilitário DIG. No capítulo 3, será a apresentada a *BlackURLLightList*; a sua metodologia de funcionamento; e as tecnologias envolvidas na implementação da solução. No capítulo 4, serão descritos alguns experimentos realizados utilizando a *BlackURLLightList* e os resultados serão analisados e comparados com a atual *URLBlackList*. No capítulo 5, será apresentada a documentação do sistema utilizando a *Unified Modeling Language* (UML). No capítulo 6, os manuais de utilização e de instalação são

disponibilizados. A conclusão será apresentada no capítulo 7; e, por fim, as referências bibliográficas utilizadas no desenvolvimento do projeto são mostradas.

2 Revisão Bibliográfica

Neste capítulo serão apresentados os conceitos básicos necessários para o entendimento deste projeto. Na seção 2.1 serão apresentados o *Domain Name System* (DNS) e o serviço *OpenDNS* de resolução de domínio público que adiciona recursos extras ao DNS; na seção 2.3 é apresentado a *URLBlackList*; e por fim, será apresentado o utilitário *dig*.

2.1 Domain Name System (DNS)

O DNS é um serviço de gerenciamento de nomes de domínios na internet responsável pela tradução de um nome de domínio em um número de IP e vice-versa. Para que seja possível acessar alguma página na *internet* é necessário possuir o endereço do *Internet Protocol* (IP) desta página. Contudo, esse endereço é em formato numérico com até 12 caracteres (*Internet Protocol version 4 - IPv4*), dificultando a memorização do endereço das páginas. Dessa forma, o DNS mantém um banco de dados associando cada IP com um nome de domínio (por exemplo, o IP 200.9.149.88 possui o nome de domínio *cefet-rj.br*), sendo necessário apenas memorizar o domínio para acesso a página (MORIMOTO, 2009).

Fisicamente, o DNS é uma rede de servidores que possui os registros de domínios e IP existentes no planeta. Ao se tentar resolver um domínio qualquer, o pedido será encaminhado para um servidor DNS que irá verificar se aquele domínio está registrado nele. Caso o domínio não seja encontrado, ele reencaminhará o pedido ao próximo servidor e assim em diante. Atualmente, existem treze servidores DNS raiz no mundo: dez nos EUA, dois na Europa e um na Ásia. Porém, existem réplicas em diversos países com o intuito de agilizar o serviço de resolução de domínios (MORIMOTO, 2009).

Para facilitar a resolução de domínio, o DNS adota um padrão hierárquico de formação e delegação dos nomes de domínio. A estrutura se inicia com o servidor raiz e é seguido de termos como: *com*, *edu*, *gov*, *br*, *fr*, *pt*, etc. Ao se tentar resolver o domínio *noticias.cefet-rj.br*, primeiramente o servidor raiz verificará que existe uma estrutura hierárquica *br* associada a ele. Em seguida, ele encaminhará para o servidor que contém os domínios para esse nível da hierarquia, e assim por diante. A figura 1 exibe a hierarquia do domínio para este exemplo.

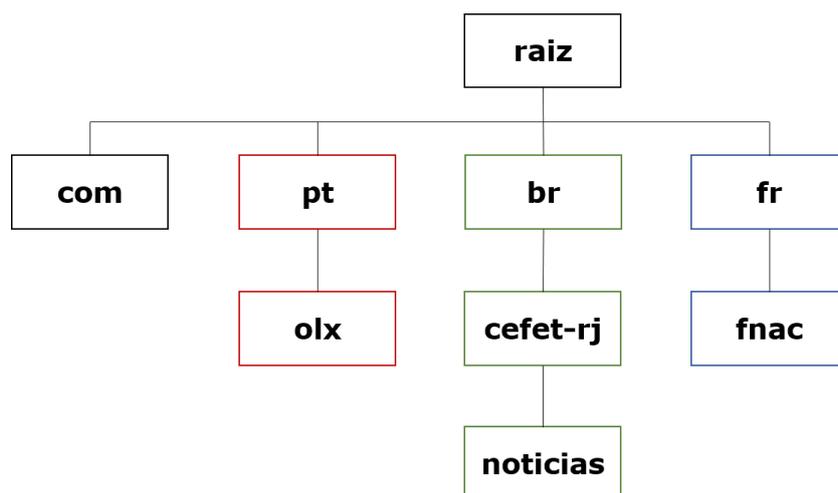


Figura 1. A hierarquia do DNS para o domínio *noticias.cefet-rj.br*.

O DNS surgiu a partir de uma demanda do crescimento da rede ARPANET nos anos 70, que usava um arquivo de texto para endereçamento dos *hosts* de sua rede. A cada inclusão de um

novo *host* na rede da ARPANET, o arquivo de texto deveria ser atualizado com as novas informações e não poderia utilizar nomes previamente já existentes. Com o crescimento e o sucesso da ARPANET, a utilização do arquivo de texto começou a gerar problemas de conflitos de nomes e de tamanho. Em 1983, Mockapetris propôs o DNS no documento *Request For Comments* (RFC) 882 e 883 (FOROUZAN, 2008).

Existem diversos servidores de DNS públicos que introduzem funcionalidades extras ao serviço de resolução de domínios como o *OpenDNS* e o *Google Public DNS*. Esses serviços são alternativas de servidores DNS, em caso de não se querer utilizar o servidor de um determinado provedor ou não implementar o serviço em uma empresa. O *OpenDNS* foi criado em 2005 e possui servidores em diversos locais do mundo (contudo não possui servidores na América do Sul). Os serviços adicionados ao DNS são: segurança contra *phishing*; auto-correção de pequenos erros ortográficos; e controle parental para bloqueio de páginas com conteúdo adulto (OPENDNS, 2015). Já o *Google Public DNS* foi lançado em 2009 e não usa nenhum serviço de redirecionamento como propaganda, além de utilizar diversos dispositivos de segurança (contra o ataque de negação de serviço por exemplo) (GOOGLEPUBLICDNS, 2015).

2.2 URLBlackList

Uma *blacklist* ou lista de bloqueio é um conjunto de elementos que possuem acesso negado a determinado serviço. Para domínios da internet existe a *URLBlackList*, que é uma lista de catalogação de domínios dividida em diversas categorias. Atualmente, a lista possui cerca de 100 categorias e 3.859.857 entradas. A lista de categorias existentes na *URLBlackList*, atualmente, pode ser encontrada no Anexo I. O processo de catalogação da *blacklist* pode ser feito por solicitação direta pelo site www.urlblacklist.com ou por pedido dos clientes e é disponibilizada com uma periodicidade de 15 dias (URLBLACKLIST, 2015). O arquivo consiste de um conjunto de diretórios separados em categoria com os seguintes arquivos sem tipo em cada diretório: um arquivo com todos os domínios da categoria (um por linha); um arquivo de URL por linha de determinada categoria; e um arquivo de expressões (palavras) separadas por uma barra vertical. Um exemplo de uma lista da *URLBlackList* pode ser visto na figura 2.



Figura 2. O conteúdo da categoria adult.

A *URLBlackList* pode ser utilizada em conjunto com um servidor *Proxy*, que é responsável por intermediar os acessos entre o usuário e a internet. Esse servidor permite que a *URLBlackList* possa ser utilizada na configuração de regras de acessos definidas por um administrador de redes. Este projeto utiliza a *URLBlackList* por ser uma das listas de bloqueios mais extensas; bem aceita na comunidade; e a lista é um serviço comercial que possui uma versão gratuita para *download*.

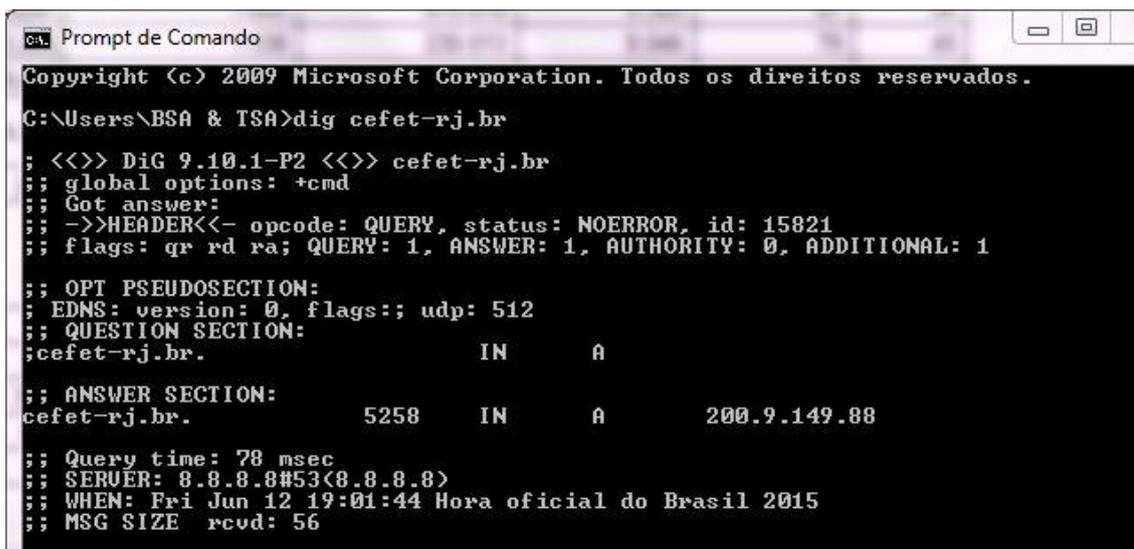
2.3 DIG

O *Domain Information Groper* (DIG) é um utilitário de linha de comando responsável por verificar nome de servidores DNS tanto no *Linux* quanto no *Windows* e faz parte do pacote *Berkeley Internet Name Domain* (BIND), que é um pacote de implementação de protocolos de DNS. O BIND foi desenvolvido na Universidade da Califórnia no início dos anos 80 e atualmente está na versão 10.2 (BIND, 2015).

O DIG possui a seguinte sintaxe: *dig [servidor] [nome] [tipo]*. O *servidor* é o nome ou endereço IP do servidor que se deseja utilizar na consulta; o campo *nome* é o domínio a ser procurado; o campo *tipo* indica o tipo da consulta a ser executada. As consultas mais utilizadas podem ser dos seguintes tipos:

1. A, que é o endereço de IP;
2. ANY, que pode ser qualquer tipo;
3. MX, que consulta servidores de *e-mail*;
4. NS, que consulta o nome dos servidores.

Por exemplo, ao rodar *dig cefet-rj.br* é retornado no campo *got answer* (indicando a resposta) um indicador chamado *ANSWER*, que representa se o domínio foi resolvido ou não. Caso o valor desse indicador for igual a 0, indica que o domínio não resolve (nenhum IP associado ao domínio), enquanto que se este for diferente de 0, indica que o domínio resolve (retornando a quantidade de IP associado ao domínio). Na seção *ANSWER SECTION*, aparecem os IP associados ao domínio consultado e em seguida o tempo de resposta. A figura 3 exibe a execução do DIG para o domínio *cefet-rj.br*.



```
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.
C:\Users\BSA & TSA>dig cefet-rj.br
;; <<>> DiG 9.10.1-P2 <<>> cefet-rj.br
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 15821
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 512
;; QUESTION SECTION:
;cefet-rj.br.                IN      A
;; ANSWER SECTION:
cefet-rj.br.                5258    IN      A      200.9.149.88
;; Query time: 78 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Jun 12 19:01:44 Hora oficial do Brasil 2015
;; MSG SIZE rcvd: 56
```

Figura 3. O dig para o domínio cefet-rj.br.

Agora, ao executar *dig sportal.co.uk*, no campo *got answer* o indicador *ANSWER* é igual a 0, indicando que não existe IP associado aquele domínio, ou seja, o domínio não resolve. Nesse caso, a seção *ANSWER SECTION* não aparece nos resultados obtidos pelo comando. Na figura 4 é possível ver o *prompt* de comando com a execução e o resultado do DIG.

```
ca. Prompt de Comando
C:\Users\Carlos>dig sportal.co.uk

;; <<>> DiG 9.10.1-P2 <<>> sportal.co.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34683
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 512
;; QUESTION SECTION:
;;sportal.co.uk.                IN      A

;; AUTHORITY SECTION:
sportal.co.uk.                1799    IN      SOA     ns1.netnames.net. hostmaster.net
names.net. 2013062001 10800 1800 3600000 21600

;; Query time: 336 msec
;; SERVER: 8.8.8.8#53<8.8.8.8>
;; WHEN: Fri Jun 12 20:54:03 Hora oficial do Brasil 2015
;; MSG SIZE rcvd: 105

C:\Users\Carlos>
```

Figura 4. O dig para um domínio que não resolve.

O DIG foi utilizado neste projeto para servir como ferramenta de resolução de domínio, onde é verificado o valor do campo *ANSWER* para sinalizar se o domínio foi ou não resolvido (0 ou outros). O DIG foi escolhido pois ele permite identificar de forma clara a resposta de resolução do domínio, além disso, o DIG é um utilitário pertencente ao protocolo de DNS, uma vez que está sendo utilizado o próprio DNS para consultas, é recomendado a utilização de um pacote nativo.

3 BlackURLLightList

Neste capítulo serão apresentados os métodos e as etapas utilizadas para solucionar os problemas identificados na *URLBlackList*. Sendo assim, os processos usados para gerar a lista enxuta irão:

1. Eliminar os IP existentes dentro das listas de domínio da *URLBlackList*;
2. Segmentar a *URLBlackList* em domínios resolvíveis e não resolvíveis;
3. Tratar os domínios com formatos ilegais e as anomalias de resolução;
4. Analisar e tratar os domínios redundantes encontrados em mais de uma categoria;
5. Adequar o contexto americano das categorias à cultura brasileira.

Dessa forma, o conjunto de processos abordados neste capítulo será capaz de gerar a *BlackURLLightList*, que é uma lista de catalogação enxuta, composta apenas por domínios resolvíveis, não redundantes e livre de qualquer anomalia. Além disso, as categorias da *BlackURLLightList* estarão adequadas ao contexto cultural brasileiro. Quando um servidor *Proxy* utilizar a *BlackURLLightList* como base para o serviço de controle de conteúdo não haverá o desperdício de tempo e nem de recursos computacionais ocasionado pelos problemas apontados na *URLBlackList*. Dessa forma, a lista *BlackURLLightList* será o produto gerado por esses processos a fim de solucionar os problemas descritos.

Para o melhor entendimento, a descrição da metodologia utilizada no projeto *BlackURLLightList* será dividida em três processos (Processo de Refinamento; Processo de Análise de Redundância; Processo de Reclassificação das Categorias). Os processos de refinamento e análise de redundância serão os responsáveis por refinar, tratar e gerar a *BlackURLLightList*, enquanto que o processo de reclassificação irá adequar a catalogação da *URLBlackList* ao contexto brasileiro. Na seção 3.1 será apresentada a metodologia da ferramenta *BlackURLLightList* e seus processos associados; e na seção 3.2 serão apresentadas as tecnologias e a forma como a ferramenta foi desenvolvida.

3.1 A Metodologia

A metodologia da *BlackURLLightList* abrange três processos, que em conjunto realizam o processo da geração de uma lista de catalogação enxuta. Primeiramente, a *URLBlackList* servirá como entrada para o processo de refinamento, para que todos os IP encontrados sejam expurgados, a segmentação dos domínios em resolvíveis e não resolvíveis seja realizada e os domínios com formatos ilegais e com anomalias de resolução sejam identificados e também expurgados. Para isso, esse processo será realizado em duas etapas. A primeira etapa é a identificação dos IP e a segunda etapa é a resolução de domínio. Após essas etapas, os domínios refinados serão armazenados pertencendo ao segmento resolvível ou não resolvível de uma categoria.

O processo de refinamento segue sequencialmente as duas etapas quando novos domínios entram como *input* do processo de refinamento. Dessa maneira, quando um domínio já existente no armazenamento entrar no processo de refinamento, este será direcionado para o processo de análise de redundância. Esse processo tem como objetivo tratar as redundâncias dos domínios pertencentes a mais de uma categoria na *URLBlackList*. Após esse processo, um domínio estará associado a apenas uma categoria segundo critérios especificados pelo Administrador de Redes. Dessa forma, quando o servidor *Proxy* utilizar a *BlackURLLightList* não terá que verificar duas ou mais vezes um mesmo domínio. A figura 5 ilustra o processo de refinamento evidenciando as etapas que um domínio percorre até chegar ao final do processo.

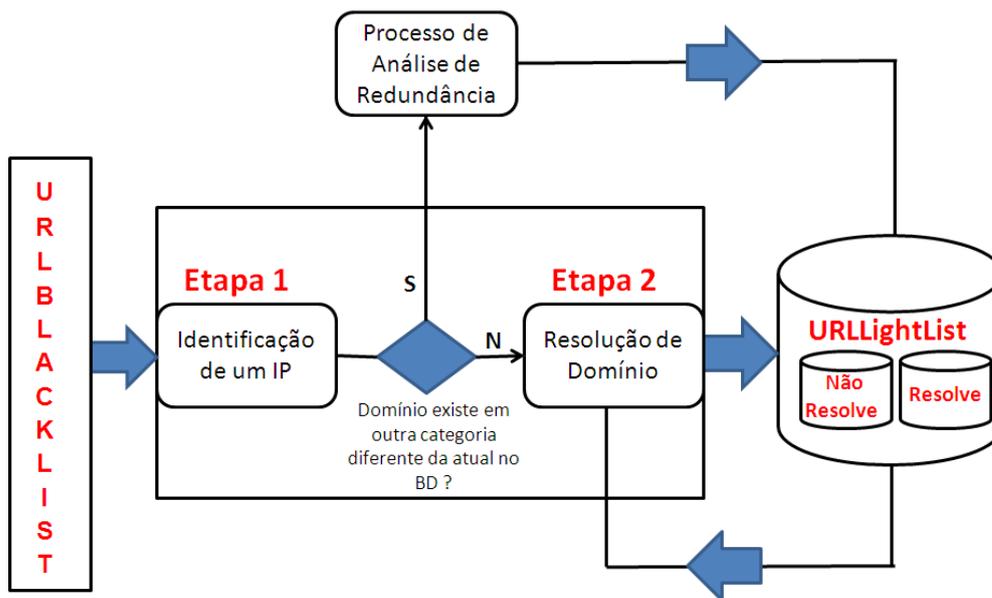


Figura 5. A metodologia da BlackURLLightList.

O último processo utilizado para a solução do problema é o processo de reclassificação de categorias. Este processo é aplicado às categorias da *URLBlackList* com o objetivo de que as categorias da *BlackURLLightList* estejam adequadas ao contexto brasileiro eliminando distorções de entendimento.

3.1.1 Processo de Refinamento

O processo de refinamento consiste na análise sequencial dos domínios pertencentes à *URLBlackList*, usando um comando específico para a resolução de domínio, com o objetivo de segmentar a lista da *URLBlackList* em dois grupos de domínios distintos: os domínios resolvíveis e os não resolvíveis. Esse processo tem como *input* a *URLBlackList* descompactada e recebe para processamento um domínio por vez. O processo de refinamento é dividido em duas etapas que serão detalhadas a seguir.

A identificação dos IP é a primeira etapa do processo. Esta etapa visa identificar e expurgar os IP presentes nas listas de domínio da *URLBlackList*. Para isso, todos os registros da *URLBlackList* passam, inicialmente, por esta etapa, a fim de impedir que IP sejam resolvidos e pertençam a uma lista que deveria conter apenas domínios. Sendo assim, essa primeira etapa realiza uma preparação para que apenas domínios prossigam para a próxima etapa.

Após a saída da primeira etapa, é identificado se um domínio já existe no armazenamento. Se o domínio não existir no armazenamento, o mesmo é direcionado para a segunda etapa do processo de refinamento. Se for identificado que esse domínio já existe no armazenamento, ele é direcionado para o processo de análise de redundância que o receberá como *input* para realizar o seu processamento.

A resolução de domínio é a segunda etapa do processo de refinamento e pode receber como *input* os domínios oriundos de dois casos distintos. O primeiro caso corresponde aos domínios que passaram pela etapa de identificação de IP e não existem no armazenamento. Neste caso, estes domínios são submetidos à etapa de resolução de domínio e se houver uma resposta do comando de resolução (não ocorrer erros), então estes domínios serão direcionados para o armazenamento, sendo relacionados a um dos segmentos (resolvíveis ou não resolvíveis) de

uma categoria. Essa distinção de segmentos possibilita a geração da *BlackURRLightList*, que será composta apenas por domínios resolvíveis que serão identificados através dessa segmentação.

Se houver uma ocorrência de erro no processo resolução de um domínio, será informado que esse domínio possui um formato ilegal ou possui qualquer outra anomalia de resolução. Dessa maneira, esses domínios serão expurgados a fim de se evitar que os mesmos façam parte da lista da *BlackURRLightList*. O resultado desse primeiro caso de *input* da etapa de resolução de domínio é uma lista enxuta, livre de anomalias e composta por dois segmentos distintos, os domínios resolvíveis e os domínios não resolvíveis.

O segundo caso da etapa de resolução de domínio recebe para processamento os domínios que estão no banco de dados de domínios chamado de *BlackURRLightList* (Figura 5), a fim de manter atualizado o *status* de resolução dos domínios. Neste caso, cada domínio armazenado passa um a um pela etapa de resolução de domínio e após o processamento esse domínio pode mudar de um segmento resolvível para um não resolvível e vice e versa, dependendo da resposta encontrada. É importante ressaltar que esse processamento não realiza nenhum expurgo, apenas atualiza o *status* de resolução dos domínios.

3.1.2 Processo de Análise de Redundância

O processo de análise de redundância é acionado quando for verificado que um domínio já existe no banco de dados associado à outra categoria diferente da atual. Após a primeira etapa do processo de refinamento, um mecanismo de identificação de domínios já existentes no armazenamento é realizado direcionando os domínios redundantes para o processo de análise de redundância. Dessa forma, esse processo tem por objetivo tratar as redundâncias de um domínio que estão associados a mais de uma categoria na *URLBlackList*, evitando assim, que um servidor *Proxy* verifique o mesmo domínio mais de uma vez.

O método de tratamento de redundância será embasado na atribuição de pesos para cada categoria existente na *URLBlackList*. O peso é um valor numérico associado à categoria e que representa o grau de perversidade dessa categoria. Entende-se por grau de perversidade: o quão perverso representa o conteúdo das páginas *web*, localizadas por domínios de uma categoria, em relação às políticas de acesso definidas por um Administrador de Redes para uma determinada rede local.

Em um ambiente escolar, por exemplo, as políticas de acesso não permitirão o acesso a domínios pertencentes a categorias como *Porn*, *Adult*, *Sexuality*, *Violence*, *Alcohol* e *Aggressive*. Portanto, categorias como essas recebem do Administrador de Redes como peso um valor entre 7 e 10, o que significa que é inadmissível pelas políticas de acesso que um usuário acesse esse tipo de conteúdo, pois são considerados perversos.

Dentro desse mesmo contexto escolar, os domínios pertencentes a categorias como *Games*, *Online Games*, *Social Networking*, *Magazines* disponibilizam conteúdos com acesso permitido pelas políticas de acesso, mas com possíveis restrições de horário. Sendo assim, essas categorias recebem do Administrador de Redes como peso, um valor entre 5 a 6, pois o acesso a esse conteúdo é admissível pelas políticas de acesso mesmo contendo certas restrições. O grau de perversidade dessas categorias é considerado moderado.

Por fim, um último grupo de categorias recebe do Administrador de Redes como peso um valor entre 1 e 4, o que significa que de acordo com as políticas de acesso definidas para este ambiente escolar, os acessos aos domínios pertencentes a essas categorias serão permitidos. Nesta faixa de peso, o Administrador de Redes não possui nenhuma preocupação em relação ao acesso do usuário a esses conteúdos, pois o grau de perversidade é baixo ou nulo. Por exemplo, as categorias *Religion*, *Books*, *Cooking*, *Child* e *Child Care* pertencem a esse grupo.

Após atribuir o grau de perversidade às categorias, relacionando as políticas de acesso que devem ser respeitadas às faixas de peso, o processo estará configurado de forma criteriosa para

realizar a análise de redundância. Esse processo consiste em comparar o grau de perversidade atribuído a cada categoria quando um domínio redundante for encontrado. Para facilitar a compreensão, o domínio *sexinfo101.com* que se encontra na lista de domínio de três categorias diferentes da *URLBlackList* (*Porn*, *Sexuality* e *Adult*) será utilizado como *input* para o processo de análise de redundância.

Supondo que o Administrador de Redes tenha atribuído os seguintes valores 9, 10 e 10 como peso para as respectivas categorias *Sexuality*, *Porn* e *Adult*; e que a análise de redundância ocorra na mesma ordem. A primeira vez que o domínio *sexinfo101.com* passar pelo processo de refinamento sendo associado à categoria *Sexuality*, esse domínio será resolvido e direcionado para o armazenamento pertencendo ao segmento de domínios resolvíveis da categoria *Sexuality*.

Na segunda vez que o domínio *sexinfo101.com* passar pelo processo de refinamento associado à categoria *Porn*, este domínio não será submetido à etapa de resolução de domínio, entretanto, este será direcionado para o processo de análise de redundância. Neste processo, a categoria que possui o maior grau de perversidade (peso) prevalecerá sobre a categoria com menor grau de perversidade. Logo, ocorrerá uma mudança em relação à categoria do domínio *sexinfo101.com*, que agora estará associado à categoria *Porn*, pois esta tem o maior grau de perversidade.

A terceira vez que o domínio *sexinfo101.com* passar pelo processo de refinamento agora associado à categoria *Adult*, este será novamente direcionado para a análise da redundância. Neste caso, o domínio não irá mudar de categoria, pois o grau de perversidade das categorias é o mesmo. Por consequência ao final do processo de refinamento, o domínio *sexinfo101.com* estará associado somente à categoria *Porn*, eliminando assim, as redundâncias existentes.

3.1.3 Processo de Reclassificação de Categorias

O processo de reclassificação de categorias recebe como *input* as categorias da *URLBlackList* e tem como objetivo possibilitar a correção de certas distorções de entendimento relacionadas a interpretação do significado de cada categoria. Isso ocorre porque as categorias da *URLBlackList* estão atreladas a linguagem e a cultura americana e por isso, quando traduzidas para a linguagem e a cultura brasileira sofrem certas distorções de entendimento. Esse processo possibilitará que as categorias da *BlackURLLightList* estejam concisas conforme a especificidade cultural brasileira.

Por exemplo, a categoria *Guns* faz referência às armas de pequeno porte que são comercializadas livremente nos Estados Unidos, já a categoria *Weapons* contempla artefatos de guerra, cuja portabilidade não é permitida. No Brasil, não existe essa distinção e qualquer porte de arma deve passar por um processo de legalização. Logo, não faz sentido a existência de duas categorias que correspondem à mesma interpretação no contexto brasileiro. Outro exemplo envolve o par das categorias *Cooking* e *Culinary* e o par das categorias *Banking* e *Bank* que também não possuem distinção de significado.

Esse processo possibilita que o Administrador de Redes escolha as categorias que, segundo a sua avaliação, devem ser unificadas em uma única categoria devido ao contexto a que se referem. Sendo assim, esse processo receberá uma lista de categorias selecionadas pelo Administrador de Redes e entregará como resultado uma única categoria, nomeada de forma a atender a interpretação do significado e que possui como lista de domínios o conjunto dos domínios pertencentes a cada categoria que foi unificada. Dessa maneira, aplicando esse processo as categorias *Guns* e *Weapons* o resultado obtido é a criação de uma categoria chamada de *Armas* pelo Administrador de Redes e que possui como lista de domínio, o conjunto de domínios pertencentes às categorias *Guns* e *Weapons*.

Por consequência, esse processo facilitará o trabalho de configuração de regras de acesso pelo Administrador de Redes que poderá utilizar uma única categoria para restringir o acesso a categorias com significados semelhantes. Por exemplo, ao invés ter que definir uma regra com

duas categorias (*Games* e *Online Games*), para bloquear o acesso ao conteúdo de jogos, o Administrador de Redes definirá a regra de acesso com apenas uma categoria unificada chamada de *Jogos*.

3.2 Implementação da BlackURLLightList

A *BlackURLLightList* é uma ferramenta *web* responsável por gerar uma lista enxuta, chamada de *BlackURLLightList* tendo como *input* para o processo de refinamento a lista da *URLBlackList*. A ferramenta é um conjunto de páginas *Java Server Pages* (JSP) composta por um menu na área administrativa onde é possível cadastrar domínios e administrador; gerenciar o grau de perversidade das categorias, bem como os registros de domínio e de administrador; gerar a *BlackURLLightList* dos domínios resolvíveis e a dos domínios não resolvíveis; analisar o arquivo da *URLBlackList* e analisar os domínios no banco de dados da *URLBlackList*.

A ferramenta foi implementada utilizando as tecnologias: *Java Enterprise Edition* (EE) para o desenvolvimento das páginas *web*; para o banco de dados relacional foi utilizado o servidor *MySQL*; o *Hibernate* foi utilizado como ferramenta de mapeamento objeto relacional para facilitar o acesso ao banco de dados; o *Gson* foi usado para serializar um objeto em *Java* para *JSON*; o *AJAX* para a realização de chamadas assíncronas e síncronas entre as diversas páginas do sistema; o *Log4j* para escrever todas as mensagens em um arquivo de *log*; o *JDOM* para a manipulação de arquivos em *XML*.

O *Java EE* é uma plataforma de desenvolvimento de aplicações que estende a utilização da linguagem *Java* (*Micro Edition* e *Standard Edition*) com objetivo de criar softwares executados no lado do servidor. Atualmente o *Java EE* é utilizado para a construção de páginas dinâmicas na *Internet* que representam sistemas de informações institucionais com manipulação de informações através da utilização de banco de dados. Popularmente o *Java EE* é conhecido como *Java Web*.

O *Java EE* utiliza *Java Server Pages* (JSP), que são páginas dinâmicas com conteúdo *HTML* e *Java*, onde o conteúdo em *Java* é processado no lado do servidor e é retornado estaticamente em conteúdo *HTML*. No lado do cliente, as informações são transformadas e exibidas por um navegador. Uma outra solução disponível é a *Servlet*, que é uma classe *Java* que trata de requisições do protocolo *HTTP* para processar dinamicamente o conteúdo e roda diretamente em um servidor *web*. Para serem executadas, as *Servlets* precisam de um *container web*.

As páginas em *JSP* e as *Servlets* também podem acessar um banco de dados residente em um Sistema Gerenciador de Banco de Dados (SGBD) através de um conector *Java DataBase Connector* (*JDBC*). A arquitetura Cliente-servidor descrita pode ser vista na Figura 6.

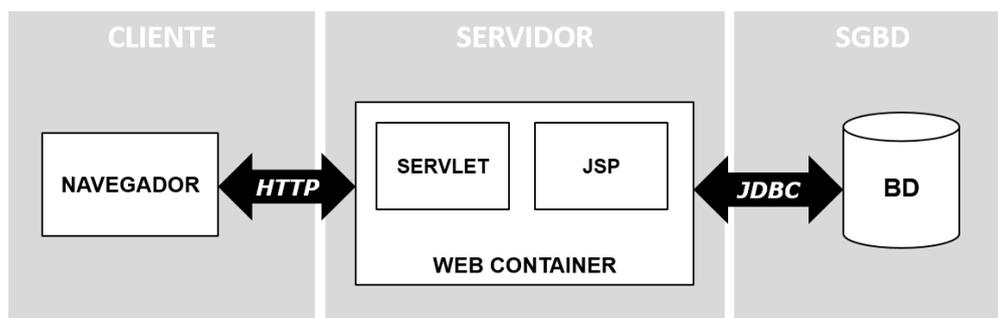


Figura 6. A arquitetura Cliente-servidor.

Para se criar e manter as páginas *JSP* é necessário um servidor *web* com suporte a *servlets* (também chamado de *container web*). Existem diversas tecnologias dão este tipo de suporte às aplicações *Java EE* como o *Apache Tomcat*, *Apache Geronimo*, *GlassFish* e *Jetty*. Nesse trabalho foi utilizado o *Apache Tomcat*.

Algumas ferramentas foram desenvolvidas para facilitar o acesso ao banco de dados, de forma a melhorar a transição de dados utilizados por um objeto ao um modelo tabular manipulado pelo banco de dados ou vice-versa. Essas ferramentas realizam um trabalho de mapeamento com acesso ao banco de dados, funcionando como um intérprete entre o banco de dados e as classes da camada de modelo. Uma das ferramentas de mapeamento existentes é o *Hibernate*.

O *Hibernate* é um *framework* que se relaciona com o banco de dados por intermédio de um mapeamento objeto/relacional para Java. Dessa forma a responsabilidade de gerenciar o acesso ao banco de dados é entregue ao *Hibernate*. Com isso, o *Hibernate* simplifica as classes pertencentes à camada de acesso a dados, ou o *Data Access Object* (DAO), já que a ferramenta gerencia a transição de informações das classes para o banco de dados ou do banco de dados para as classes. Em poucas linhas de código essa transição é realizada, permitindo que o programador dedique mais tempo construindo a lógica do negócio. Esse projeto utilizou o *framework Hibernate* com a abstração fornecida pelo uso de coleções, proporcionando assim, flexibilidade dos métodos de acesso ao banco de dados.

O padrão de *software Model-View-Controller* (MVC) foi utilizado no desenvolvimento da ferramenta *BlackURLLightList* proporcionando uma separação do sistema em camadas. O padrão consiste em dividir uma aplicação em três partes interligadas, separando as regras do negócio do sistema modelado da forma como este será exibido para o usuário. Em outras palavras, o padrão MVC permite que o usuário tenha acesso apenas às informações processadas pelo servidor sem ter acesso direto a lógica de negócio. Essa separação facilita a manutenção do sistema e a inclusão de novas funcionalidades (KRASNER, POPE, 1988).

4 Análise dos Experimentos

Neste capítulo serão apresentados os resultados obtidos com os experimentos realizados com a ferramenta *BlackURLLightList*. Os experimentos foram realizados com o objetivo de proporcionar uma análise comparativa entre as listas da *URLBlackList* e da *BlackURLLightList*, comprovar a compatibilidade de execução da ferramenta nos os sistemas operacionais *Windows* e *Linux* e para demonstrar o índice de redução dos registros de domínios da *URLBlackList*.

4.1 Análise

Os primeiros experimentos foram realizados no sistema operacional *Linux* devido ao fato do comando de resolução de domínio utilizado pela ferramenta, o DIG, pertencer ao pacote de utilitários desse sistema operacional. Durante os experimentos, estudos eram feitos em busca de uma solução para que a *URLLightList* pudesse ser executada também no sistema operacional *Windows*. É importante ressaltar que nenhum problema foi registrado nessa fase e a ferramenta em execução se mostrou viável como solução proposta. Nessa experimentação inicial, a necessidade de que o sistema registrasse todo o seu funcionamento em um *log* foi evidenciada a fim de capturar qualquer comportamento desconhecido. Ainda sobre essa fase, a primeira versão da *BlackURLLightList* foi implementada utilizando o *Java Standard Edition* (SE) como tecnologia de desenvolvimento e o experimento foi executado via terminal do sistema operacional *Linux*.

Em uma segunda fase de experimentação, a *BlackURLLightList* teve o seu funcionamento verificado no ambiente *Windows* através da instalação do utilitário DIG neste sistema operacional. A ferramenta realizou o processo de refinamento da *URLBlackList* conforme o esperado, entretanto, a falta de energia durante os experimentos apontou a necessidade de que fosse implementado um mecanismo para reiniciar uma análise interrompida. Depois que esses experimentos foram realizados, a *BlackURLLightList* teve a compatibilidade de execução nos sistemas operacionais *Linux* e *Windows* devidamente comprovada. Além disso, nessa segunda fase ocorreu a migração de tecnologia utilizada na ferramenta de *Java Standard Edition* (JSE) para *Java Enterprise Edition* (JEE).

A tabela 1 e as tabelas de Resultado Obtido por Categoria (Anexo II) foram criadas para demonstrar os resultados obtidos em um processo de refinamento realizado pela *BlackURLLightList* tendo como *input* a lista da *URLBlackList*. Os resultados apresentados nestas tabelas foram computados do último experimento realizado utilizando uma versão da *URLBlackList* disponibilizada em 14 de maio de 2015. O processo foi executado em aproximadamente cinco dias e analisou noventa e nove categorias e 2.901.374 domínios presentes nessa versão da *URLBlackList*.

<i>URLBlackList</i>	2.901.374	100%
BlackURLLightList Resolúvel	1.202.452	41,44%
BlackURLLightList Não Resolúvel	756.096	26,06%
Domínios com formato ilegais/redundantes/IP	942.826	32,50%
Índice redução (%)	58,56%	

Tabela 1. Resumo dos Resultados Obtidos.

O índice *URLBlackList* representa a quantidade de domínios encontrados na lista da *URLBlackList*; já o índice *BlackURLLightList – Resolúvel* representa o quantitativo de domínios resolvíveis identificados na lista da *URLBlackList* pelo processo de refinamento da *BlackURLLightList*; o índice *BlackURLLightList – Não Resolúvel* representa o quantitativo de domínios não resolvíveis identificados na lista da *URLBlackList*; o índice de domínios com formato ilegais/redundantes/anômalos/IP engloba a quantidade de domínios que foram

expurgados durante a etapa de resolução de domínio por possuírem formatos ilegais ou outras anomalias encontradas, a quantidade de IP expurgados pela primeira etapa do processo de refinamento e a quantidade de redundâncias tratadas, pois agora um domínio pertence a apenas uma categoria; e por fim, o índice de *redução* representa o percentual de registros retirados da *URLBlackList* revelando assim, o quanto a lista ou uma categoria ficou mais enxuta após o processo de refinamento da *BlackURLLightList*.

A tabela 1 representa o resultado geral do processo de refinamento. No total, a ferramenta *BlackURLLightList* processou 2.901.374 domínios pertencentes à *URLBlackList* e 756.096 desses domínios foram identificados como não resolvíveis, logo, não precisariam ser verificados pelo servidor *Proxy* desperdiçando os recursos computacionais. Nesta análise, percebemos que a *BlackURLLightList* proporcionou uma redução de cerca de 26 % em relação a lista da *URLBlackList*. Sendo assim, retirando os domínios não resolvíveis dos registros da *URLBlackList*, esta passou a ter 2.145.278 registros.

O quarto índice dessa tabela, representa uma redução de 32,5 % nos registros da *URLBlackList* através do tratamento de redundância aplicado segundo os graus de perversidade (pesos) atribuídos à categoria conforme demonstrado na tabela do Anexo III. Esse índice também abrange a quantidade de expurgos de domínios com formatos ilegais e com outras anomalias identificadas na etapa de resolução. Aplicando mais esse percentual de redução a *URLBlackList*, esta foi reduzida para 1.202.452 registros, totalizando um índice de redução de 58,5% proporcionado pelo processamento da *BlackURLLightList*.

O quarto índice dessa tabela também constata que o quantitativo de registros expurgados foi maior que o quantitativo de domínios não resolvíveis encontrados. Esses 942.826 registros encontrados no quarto índice evidencia o desperdício de recursos computacionais consumidos por um servidor *Proxy* ao percorrer duas ou mais vezes o mesmo domínio por se encontrarem em diversas categorias, os IP encontrados dentro da lista de domínio da *URLBlackList* e domínios inválidos por erros formato.

Analisando as tabelas de Resultado Obtido por Categoria (Anexo I) constata-se que: a categoria *Porn*, uma das mais utilizadas pelo Administrador de Rede, obteve como índice de redução 56 por cento sendo que a quantidade de domínio não resolvível supera a quantidade de domínios resolvível; a categoria *Translation* apresentou o menor índice de redução (1%) entre todas as categorias, a categoria *Verisign* foi reduzida em 100%, pois os dois domínios existentes nessa categoria são não resolvíveis; a categoria *Phishing* com 121.388 domínios apresentou 82.098 domínios não resolvíveis, ou seja, cerca de 67,6 dessa categoria é composta por domínios não resolvíveis e a categoria *Adult* teve um total de 528.750 registros expurgados (53% do total de seus registros) e revelou um alto índice de redundância com a categoria *Porn* conforme observado no arquivo de *log* do sistema.

Portanto, os resultados obtidos com os experimentos realizados se mostraram satisfatórios já que a *URLBlackList* foi reduzida em 58,5 %, ou seja, os resultados comprovam o fato de que se a lista da *BlackURLLightList* for usada por um servidor *Proxy* ao realizar o serviço de controle de conteúdo proporcionará a otimização dos recursos computacionais utilizados por este serviço.

5 Documentação do Sistema

Neste capítulo serão apresentados os diagramas desenvolvidos para modelagem do sistema. A UML foi utilizada para representar o sistema por ser uma linguagem de modelagem com diversos diagramas voltados a sistemas orientados a objeto. Na seção 5.1 será apresentado o mini-mundo da solução; em seguida na seção 5.2 os diagramas de casos de uso, e na 5.3 a descrição desses mesmos casos. Na seção 5.4 os diagramas de classes serão mostrados, enquanto que na seção 5.5 é apresentado o diagrama de sequência. Por fim, na seção 5.6 os diagramas de atividades serão exibidos.

5.1 Mini-Mundo

Esse projeto tem por objetivo atender algumas demandas dos Administradores de Redes relativas ao processo de controle de conteúdo usando como base a lista da *URLBlackList*. A *URLBlackList* é um serviço comercial que oferece uma lista catalogada de URL, domínios e expressões que é utilizada pelos administradores de rede na configuração dos servidores *Proxy* para realizar o controle do conteúdo das páginas *web* acessadas pelos usuários. Sobre as informações coletadas relativas à *URLBlackList* podemos enumerar:

1. Uma versão da *URLBlackList* é disponibilizada para *download* no site <http://www.urlblacklist.com/>, juntamente com um código MD5 correspondente ao arquivo;

2. A lista da *URLBlackList* é composta por várias categorias e cada categoria possui um nome e uma lista de domínio. Uma categoria só pode ser criada pelos desenvolvedores da *URLBlackList* através de uma requisição de um cliente ou por uma nova necessidade em categorizar um grupo de domínios com conteúdo semelhantes. Uma vez criada, uma categoria não pode ser excluída;

3. As categorias recebem nomes americanos de acordo com o contexto cultural;

4. Cada categoria possui vários domínios associados e um domínio pode ser encontrado em mais de uma categoria na *URLBlackList*. Um domínio só pode ser incluído, excluído ou alterado na *URLBlackList* através de uma solicitação submetida por formulário *web*. Essa solicitação pode ou não ser aprovada pela avaliação dos desenvolvedores da *URLBlackList*;

5. Existem domínios que não resolvem (inativos) nas listas de domínios da *URLBlackList*;

6. Existem IP e domínios com formatos ilegais nas listas de domínios da *URLBlackList*.

Para que o controle de conteúdo seja aplicado, um Administrador de Redes precisa configurar em um servidor *Proxy* um conjunto de regras utilizando uma lista de domínios. Cada domínio presente nas listas de domínios é percorrido e comparado pelo servidor *Proxy*. Sendo assim, é desejável pelos Administradores de Redes que as listas de domínios possuam as seguintes características:

- Que a lista seja composta somente por domínios resolvíveis, os quais realmente devem ser checados pelo servidor *Proxy*;

- Que um domínio esteja associado a apenas uma categoria, evitando redundâncias de verificação;

- Que domínios com formatos ilegais e o IP sejam retirados da lista;

- Que seja possível reclassificar as categorias, aglutinando categorias cujos contextos sejam semelhantes;

- Que seja possível inserir e modificar um domínio na lista, sem necessitar da aprovação dos desenvolvedores da *URLBlackList*.

O sistema será chamado de *BlackURLLightList* e terá como funcionalidade principal o refinamento da lista da *URLBlackList*. Para isso, o sistema deverá percorrer cada domínio existente na lista da *URLBlackList* e verificar se o mesmo é resolvível ou não. Nesta análise do arquivo da *URLBlackList*, apenas os domínios novos deverão ser resolvidos e então armazenados no banco de dados. Se um domínio já existir na base de dados, o sistema deverá analisar a redundância de domínio segundo critérios estabelecidos pelo próprio administrador a fim de não permitir que um domínio esteja associado a mais de uma categoria.

Todas as categorias encontradas na análise da *URLBlackList* deverão ser armazenadas e cada categoria possuirá um nome e uma lista de domínios. Os IP encontrados dentro da lista de domínio da *URLBlackList* deverão ser ignorados pelo sistema, ou seja, não devem ser resolvidos e nem armazenados. Já quando os domínios com formatos ilegais forem encontrados, o sistema deverá alertar ao Administrador de Redes através de uma mensagem no log do sistema. Qualquer anomalia de resolução e outras informações pertinentes também devem ser alertadas no *log* do sistema.

Quando o Administrador de Redes julgar necessário realizar uma atualização da base de dados, o *URLLightList* deverá permitir a análise de resolução dos domínios armazenados. Nesta análise, o Administrador de Redes poderá escolher entre os domínios, atualmente, resolvíveis ou não, quais gostaria de verificar e atualizar a sua resolução. Caso ocorra uma interrupção de uma das análises, de arquivo ou banco de dados, a *BlackURLLightList* permitirá a reinicialização a partir da linha onde a análise foi interrompida.

O administrador poderá realizar várias reclassificações de uma ou de várias categorias. Esta reclassificação irá gerar uma nova categoria que deverá ser nomeada pelo Administrador de Redes e que agrupará todas as listas de domínios associadas às categorias aglutinadas.

Após a análise e o refinamento da lista da *URLBlackList*, o *software* permitirá a geração da lista catalogada da *URLLightList*. Esta lista será enxuta, pois irá conter apenas os domínios, comprovadamente resolvíveis e sem redundâncias. Além disso, a lista da *BlackURLLightList* estará livre de IP e de domínios com formatos ilegais.

O sistema possibilitará a geração da *BlackURLLightList* em dois formatos. O primeiro formato de exportação que o sistema permitirá será conservando a mesma estrutura de catalogação da lista da *URLBlackList*. Já o segundo formato seguirá a catalogação das reclassificações realizadas pelo administrador, gerando assim, uma lista com as novas categorias reclassificadas e cada uma conterá um arquivo de domínio correspondente às aglutinações. A exportação de domínios inativos também será disponibilizada pelo sistema, sendo que apenas um arquivo será gerado contendo todos os domínios não resolvíveis armazenados.

A *BlackURLLightList* permitirá, ainda o cadastramento, a exclusão e a alteração de domínios no banco de dados e informará ao Administrador de Redes se existe uma nova versão da lista da *URLBlackList* disponível para que o *download* seja realizado. Por fim, o sistema deve permitir a divulgação e a distribuição da lista da *BlackURLLightList* através de um *download* solicitado por qualquer usuário, não precisando este de nenhum cadastramento ou *login*.

5.2 Diagrama de Casos de Uso

O Diagrama de Casos de Uso é um diagrama pertencente a UML, que modela as funcionalidades e comportamentos do sistema. Ele é responsável por identificar as interações de atores externos ao sistema e os casos de uso em que cada um atua. O Diagrama de Casos de Uso é utilizado durante a fase de engenharia de requisitos de um sistema (BEZERRA, 2006). O Diagrama de Casos de Uso da *BlackURLLightList* pode ser visto na Figura 7.

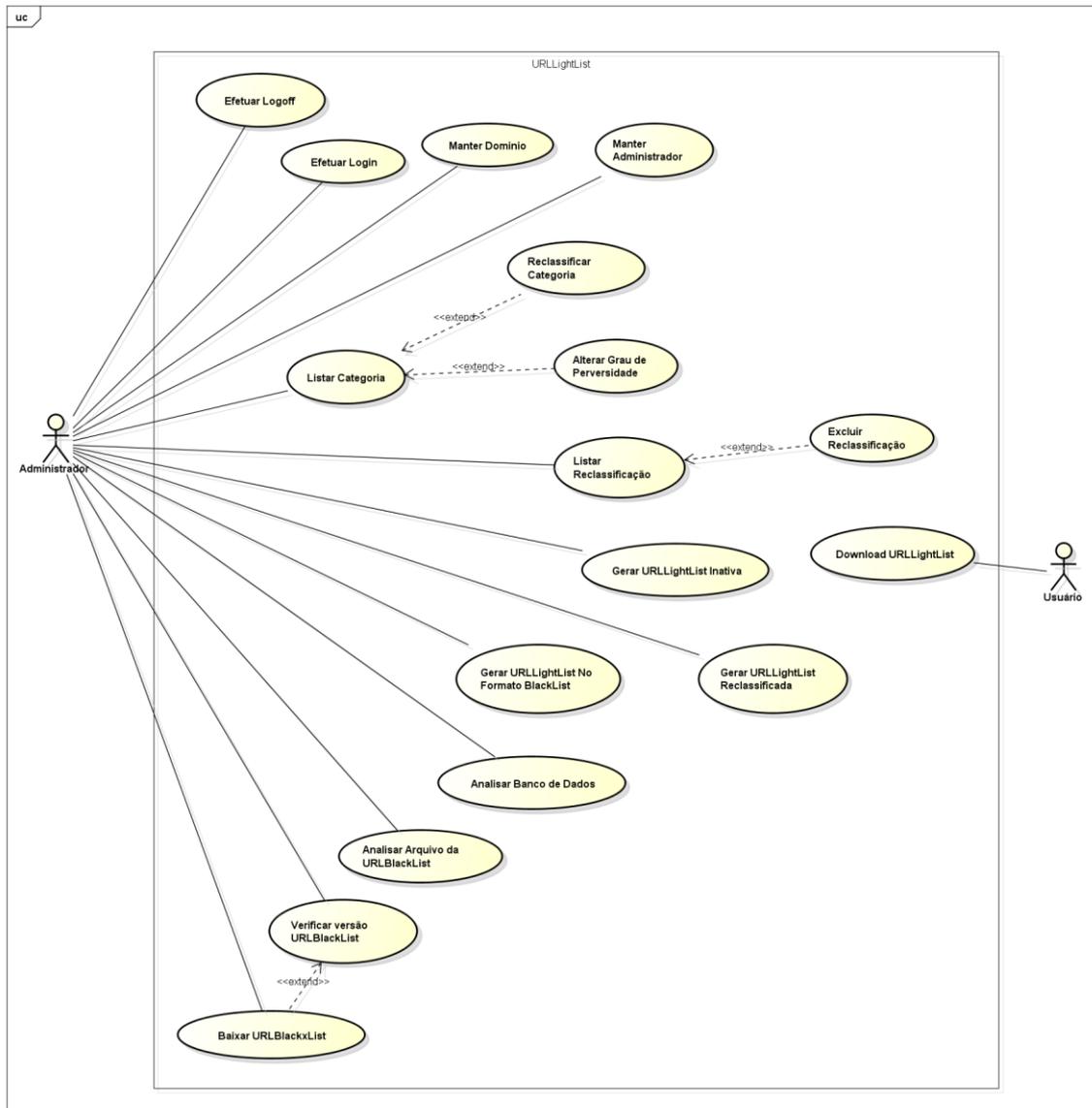


Figura 7. O diagrama de caso uso da BlackURLLightList.

5.3 Descrição de Casos de Uso

A Descrição de Casos de Uso é um documento em formato de texto onde os casos de uso previamente mapeados são documentados passo a passo. O caso descreve o que o sistema deverá fazer. Os principais campos a serem descritos em caso de uso são: a identificação do ator que inicia o caso de uso; as pré-condições; os fluxos normal, alternativo e de exceção; pós-condições; e regras de negócios (BEZERRA, 2006).

5.3.1 Caso de Uso 1 – Cadastrar Domínio

Caso de Uso 1 (CDU1)	Cadastrar Domínio		
Descrição	Permite o cadastro de um domínio no sistema.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Cadastrar" e escolhe a opção "Domínio".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela de cadastro de domínio.
	2	Informa Domínio e Categoria.	
	3	Acessa a opção "Salvar".	
	4		Realiza a validação dos dados. [RN1][RN2][RN3].
	5		Resolve o domínio.
	6		Lê a resposta de sucesso da resolução.
	7		Interpreta a resposta.
	8		Salva os dados do domínio caso o status do domínio seja ativo.
	9		Exibe a mensagem: "Cadastrado com sucesso!".
	10		Termina o caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Domínio cadastrado.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
Fluxo Alternativo 2 (FA2) – "Domínio com status não resolvível"	Ao passo 8 do FP		
	Passo	Ator	Sistema
	1		Exibe a mensagem: "Domínio não resolve, logo não pode ser salvo".
	2		Termina o caso de uso.
Fluxo de Exceção 1 (FE1) – "Erro de resolução."	Ao passo 6 do FP		
	Passo	Ator	Sistema
	1		Lê a resposta de erro da resolução.
	2		Identifica um formato inválido de domínio.
	3		Exibe a mensagem: "Um erro inesperado ocorreu!".
4		Termina a execução do caso de uso.	
Fluxo de Exceção 2 (FE2) – "Conectividade inexistente"	Ao passo 2 do FE1		
	Passo	Ator	Sistema
	1		Registra uma mensagem no arquivo de <i>log</i> informando sobre a falha de conectividade.
	2		Exibe a mensagem: "Um erro inesperado ocorreu!".
3		Termina a execução do caso de uso.	
Regras de Negócio (RN)	Código	Descrição	
	1	Todos os campos são obrigatórios.	
	2	Não deve existir um domínio cadastrado com o mesmo nome.	
	3	Somente domínios resolvíveis podem ser cadastrados.	
Observações	Essa validação permite ao administrador cadastrar um domínio pertencente a qualquer nacionalidade.		

Tabela 2. CDU1 - Cadastrar Domínio.

5.3.2 Caso de Uso 2 – Buscar Domínio

Caso de Uso 2 (CDU2)	Buscar Domínio	
Descrição	Exibe um domínio para que operações possam ser realizadas sobre ele.	
Atores	Administrador	
Inclusões	Não há.	
Extensões	[CDU3] [CDU4]	
Pré-Condições (PRE)	Não há.	
Fluxo Disparador (FD)	Passo	Sistema
	1	Acessa o menu "Gerenciar" e escolhe a opção "Domínio".
Fluxo Principal (FP)	Passo	Sistema
	1	Exibe a tela gerenciar domínio.
	2	Informa Domínio.
	3	Acessa a opção "Buscar".
	4	Busca um domínio com o nome informado.
	5	Exibe o domínio com o nome informado na tela gerenciar domínio.
	6	Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência
	1	Domínio selecionado
Fluxo Alternativo 1 (FA1) – "Alterar"	Ao passo 6 do FP	
	Passo	Sistema
	1	Acessa a opção "Alterar".
	2	Executa o [CDU3].
Fluxo Alternativo 2 (FA2) – "Excluir"	Ao passo 6 do FP	
	Passo	Sistema
	1	Acessa a opção "Excluir".
	2	Executa o [CDU4].
Regras de Negócio (RN)	Nenhum	
Observações	Nenhuma.	

Tabela 3. CDU2 - Buscar Domínio.

5.3.3 Caso de Uso 3 – Alterar Domínio

Caso de Uso 3 (CDU3)	Alterar Domínio		
Descrição	Permite a alteração da categoria associada ao domínio cadastrado.		
Atores	Administrador		
Inclusões	[CDU2]		
Extensões	Não há.		
Pré-Condições (PRE)	[CDU2-FP-POS1]		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Gerenciar" e escolhe a opção "Domínio".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Executa o [CDU2].
	2	Informa a Categoria.	
	3	Acessa a opção "Alterar".	
	4		Realiza a validação dos dados. [RN1].
	5		Atualiza o domínio.
	6		Exibe a mensagem "Atualizado com sucesso!".
	7		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Domínio alterado.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo de Exceção FE	Não há.		
Regras de Negócio (RN)	Código	Descrição	
	1	O campo categoria é obrigatório.	
Observações	Nenhuma.		

Tabela 4. CDU3 - Alterar Domínio.

5.3.4 Caso de Uso 4 – Excluir Domínio

Caso de Uso (CDU4)	Excluir Domínio		
Descrição	Permite a exclusão do cadastro de um domínio.		
Atores	Administrador		
Inclusões	[CDU2]		
Extensões	Não há.		
Pré-Condições (PRE)	[CDU2-FP-POS1]		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Ac essa o menu "Gerenciar" e escolhe a opção "Domínio".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Executa o [CDU2].
	2	Acessa a opção "Excluir".	
	3		Exclui o cadastro do domínio.
	4		Exibe a mensagem: "Domínio excluído com sucesso!".
	5		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Domínio excluído.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 2 FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo de Exceção (FE)	Nenhum.		
Regras de Negócio (RN)	Nenhuma.		
Observações	Nenhuma.		

Tabela 5. CDU4 - Excluir Domínio.

5.3.5 Caso de Uso 5 – Cadastrar Administrador

Caso de Uso 5 (CDU5)	Cadastrar Administrador	
Descrição	Permite o cadastro de um administrador.	
Atores	Administrador	
Inclusões	Não há.	
Extensões	Não há.	
Pré-Condições (PRE)	Não há.	
Fluxo Disparador (FD)	Passo	Ator
	1	Acessa o menu "Cadastrar" e escolhe a opção "Administrador".
Fluxo Principal (FP)	Passo	Sistema
	1	Exibe a tela de cadastro de um administrador.
	2	Informa Login, Senha e Confirmação de senha.
	3	Acessa a opção "Salvar".
	4	Realiza a validação dos dados. [RN1][RN2][RN3][RN4] [RN5] [RN6]
	5	Salva os dados do administrador.
	6	Exibe a mensagem: "Cadastrado com sucesso!".
	7	Termina o caso de uso.
Pós-condições do FP	Código	Descrição/Referência
	1	Administrador cadastrado.
Fluxo Alternativo 1 (FA1) – "Cancelar"	Passo	Sistema
	1	Acessa a opção "Cancelar".
	2	Exibe a tela inicial do sistema.
	3	Termina a execução do caso de uso.
Fluxo de Exceção (FE)	Não há.	
Regras de Negócio (RN)	Código	Descrição
	1	Todos os campos são obrigatórios.
	2	O login deve conter no mínimo de 6 caracteres e no máximo 12 caracteres.
	3	Não deve existir um administrador cadastrado com o mesmo login.
	4	A senha deve conter apenas números.
	5	O login deve conter 6 dígitos.
	6	O campo confirmação deve ser igual ao campo senha.
Observações	.Não há.	

Tabela 6. CDU5 - Cadastrar Administrador.

5.3.6 Caso de Uso 6 – Buscar Administrador

Caso de Uso 6 (CDU6)	Buscar Administrador		
Descrição	Exibe um administrador para que uma operação de atualização possa ser realizada sobre ele.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	[CDU7]		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Gerenciar" e escolhe a opção "Administrador".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela de gerenciar administrador.
	2	Informa Login.	
	3	Acessa a opção "Buscar".	
	4		Exibe o administrador encontrado na tela.
	5		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Administrador selecionado.	
Fluxo Alternativo 1 (FA1) – "Alterar"	Ao passo 5 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Alterar"	
	2		Executa o [CDU7].
Fluxo Alternativo 2 (FA2) – "Cancelar"	Ao passo 5 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar"	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Nenhum		
Observações	Nenhuma		

Tabela 7. CDU6 - Buscar Administrador.

5.3.7 Caso de Uso 7 – Alterar Administrador

Caso de Uso 7 (CDU7)	Alterar Administrador		
Descrição	Permite a alteração do cadastro de um administrador.		
Atores	Administrador		
Inclusões	[CDU6]		
Extensões	Não há.		
Pré-Condições (PRE)	[CDU6-FP-POS1]		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Gerenciar" e escolhe a opção "Administrador".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Executa o [CDU6].
	2	Informa o Login, Senha e Confirmação .	
	3	Acessa a opção "Alterar".	
	4		Realiza a validação dos dados. [RN1][RN2][RN3][RN4][RN5][RN6]
	5		Atualiza os dados do administrador.
	6		Exibe a mensagem: "Alterado com sucesso!".
	7		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Administrador alterado.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar"	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Código	Descrição	
	1	Todos os campos são obrigatórios.	
	2	O login deve conter no mínimo de 6 caracteres e no máximo 12 caracteres.	
	3	Não deve existir um administrador cadastrado com o mesmo login.	
	4	A senha deve conter apenas números.	
	5	O login deve conter 6 dígitos.	
	6	O campo confirmação deve ser igual ao campo senha.	
	7	Deve existir um login com a senha atual informada para que a atualização seja possível.	
Observações	Nenhuma.		

Tabela 8. CDU7 - Alterar Administrador.

5.3.8 Caso de Uso 8 – Alterar Grau de Perversidade

Caso de Uso 8 (CDU8)	Alterar Grau de Perversidade		
Descrição	Permite a alteração do grau de perversidade de uma lista de categorias.		
Atores	Administrador		
Inclusões	[CDU9]		
Extensões	Não há.		
Pré-Condições (PRE)	[CDU9-POS-1]		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Gerenciar" e escolhe a opção "Grau de Perversidade".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Executa o [CDU9].
	2	Informa o Grau de perversidade para todas as categorias que deseja alterar.	
	3	Acessa a opção "Alterar".	
	4		Realiza a validação dos dados. [RN1][RN2].
	5		Atualiza os dados de todas as categorias modificadas pelo administrador.
	6		Exibe a mensagem: "Alterado com sucesso!".
	7		Termina o caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Grau de perversidade da categoria alterado.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar"	
	2		Exibe a tela inicial do sistema.
Fluxo de Exceção (FE)	Nenhum		
	Regras de Negócio (RN)	Código	Descrição
	1	O campo grau de perversidade é obrigatório.	
	2	O Grau de Perversidade deve conter somente caracteres numéricos de 1 a 10.	
Observações	Nenhuma.		

Tabela 9. CDU8 - Alterar Grau de Perversidade.

5.3.9 Caso de Uso 9 – Listar Categoria

Caso de Uso 9 (CDU9)	Listar Categoria		
Descrição	Lista as categorias armazenadas permitindo executar outras operações.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	[CDU8] [CDU9]		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador (FD-1)	Passo	Ator	Sistema
	1	Acessa o menu "Gerenciar" e escolhe a opção "Grau de Perversidade".	
Fluxo Disparador (FD-2)	Passo	Ator	Sistema
	1	Acessa o menu "Reclassificar" e escolhe a opção "Categoria".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Busca todas as categorias.
	2		Exibe todas as categorias em uma das telas: gerenciar Grau de categoria (FD-1) e Reclassificar categoria (FD-2).
	3	Segue um dos fluxos alternativos: (FA1), (FA2).	
Pós-condições do FP	Código	Descrição/Referência	
	1	Categorias listadas.	
Fluxo Alternativo 1 (FA1) – "Gerenciar Grau de Perversidade"	Após o passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Alterar" na tela de gerenciar grau de perversidade.	
	2		Executa o [CDU8]
Fluxo Alternativo 2 (FA2) – "Reclassificar Categoria"	Após o passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Salvar" na tela de reclassificar categoria	
	2		Executa o [CDU10]
Fluxo de Exceção (FE)	Nenhum.		
Regras de Negócio (RN)	Nenhuma.		
Observações	Nenhuma.		

Tabela 10. CDU9 - Listar Categoria.

5.3.10 Caso de Uso 10 – Listar Reclassificação

Caso de Uso 10 (CDU10)	Listar Reclassificação		
Descrição	Lista as reclassificações armazenadas permitindo operações de exclusão sobre elas.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	[CDU11]		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Reclassificar" e escolhe a opção "Categoria".	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe todas as reclassificações realizadas pelo administrador na tela de reclassificar categoria.
Pós-condições do FP	Código	Descrição/Referência	
	1	Reclassificações listadas.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Após o passo 1 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar" na tela de reclassificar categoria.	
	2		Exibe a tela inicial do sistema.
Fluxo Alternativo 2 (FA2) – "Excluir Reclassificação"	Após o passo 1 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Excluir" na tela de reclassificar categoria.	
	2		Executa o [CDU11].
Fluxo de Exceção (FE)	Nenhum.		
Regras de Negócio (RN)	Nenhuma.		
Observações	Nenhuma.		

Tabela 11. CDU10 - Listar Reclassificação.

5.3.11 Caso de Uso 11 – Excluir Reclassificação

Caso de Uso 11 (CDU11)	Excluir Reclassificação	
Descrição	Permite a exclusão do cadastro de uma reclassificação.	
Atores	Administrador	
Inclusões	[CDU10]	
Extensões	Não há.	
Pré-Condições (PRE)	[CDU10-FP-POS1]	
Fluxo Disparador (FD)	Passo	Ator
	1	Acessa o menu "Reclassificar" e escolhe a opção "Categoria".
Fluxo Principal (FP)	Sistema	
	Passo	Ator
	1	Acessa a opção "Excluir".
	2	
	3	
4		
		Sistema
		Exclui o cadastro da reclassificação.
		Exibe a mensagem: "Exclusão com sucesso!".
		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência
	1	Reclassificação excluída.
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 2 FP	
	Passo	Ator
	1	Acessa a opção "Cancelar".
	2	
3		
		Sistema
		Exibe a tela inicial do sistema.
		Termina a execução do caso de uso.
Fluxo de Exceção (FE)	Nenhum.	
Regras de Negócio (RN)	Nenhuma.	
Observações	Nenhuma.	

Tabela 12. CDU11 - Excluir Reclassificação.

5.3.12 Caso de Uso 12 – Reclassificar Categoria

Caso de Uso 12 (CDU12)	Reclassificar Categoria	
Descrição	Permite o cadastro de uma reclassificação de categorias.	
Atores	Administrador	
Inclusões	[CDU9]	
Extensões	Não há.	
Pré-Condições (PRE)	[CDU9-FP-POS1]	
Fluxo Disparador (FD)	Passo	Ator
	1	Acessa o menu "Reclassificar" e escolhe a opção "Categoria".
Fluxo Principal (FP)	Passo	Ator
	1	Executa o [CDU9].
	2	Informa o Nome.
	3	Escolhe uma categoria.
	4	Acessa a opção "Adicionar".
	5	Executa o FP-POS3 a FP-POS4 até que as categorias desejadas sejam adicionadas.
	6	Acessa a opção "Salvar".
	7	
	8	
	9	
Pós-condições do FP	Código	Descrição/Referência
	1	Reclassificação cadastrada
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 6 do FP	
	Passo	Ator
	1	Acessa a opção "Cancelar".
	2	
Fluxo de Exceção (FE)	Nenhum	
	Regras de Negócio (RN)	Código
	1	Todos os campos são obrigatórios.
	2	O nome deve no mínimo de 3 caracteres e no máximo 12 caracteres.
Observações	Nenhuma.	

Tabela 13. CDU12 - Reclassificar Categoria.

5.3.13 Caso de Uso 13 – Gerar BlackURLLightList - Inativa

Caso de Uso 13 (CDU13)	Gerar <i>BlackURLLightList</i> – Inativa		
Descrição	Permite gerar um arquivo com domínios não resolvíveis.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Gerar" e escolhe a opção " <i>BlackURLLightList</i> - Inativa"	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Lista os domínios com o status de resolução inativo.
	2		Cria uma pasta com o nome "Inativa" dentro de um diretório raiz.
	3		Cria um arquivo denominado <i>domains</i> dentro diretório da pasta criada.
	4		Escreve um domínio lido dentro do arquivo <i>domains</i> .
	5		Executa o FP-POS4 até que todos os domínios da lista sejam escritos.
	6		Exibe a mensagem: "A <i>BlackURLLightList</i> -Inativa foi gerada na pasta.."
	7		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Arquivo gerado com domínios não resolvíveis.	
Fluxo Alternativo	Não há.		
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Não há.		
Observações	A <i>BlackURLLightList</i> -Inativa será criada em um diretório raiz definido pelo sistema.		

Tabela 14. CDU13 - Gerar BlackURLLightList - Inativa.

5.3.14 Caso de Uso 14 – Gerar BlackURLLightList No Formato BlackList

Caso de Uso 14 (CDU14)	Gerar <i>BlackURLLightList</i> No Formato BlackList		
Descrição	Permite gerar um arquivo com domínios resolvíveis no formato da <i>URLBlackList</i> .		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Gerar" e escolhe a opção " <i>BlackURLLightList-Ativa</i> "	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela gerar arquivo <i>BlackURLLightList</i> ativa.
	2	Informa o Nome da pasta e escolhe a opção "formato <i>URLBlackList</i> ".	
	3	Acessa a opção "Gerar".	
	4		Lista as categorias com exceção das categorias reclassificadas pelo administrador.
	5		Lista os domínios com o status de resolução ativo e que estejam associados a uma categoria lida.
	6		Cria uma pasta com nome da categoria lida dentro de um diretório raiz.
	7		Cria um arquivo denominado <i>domains</i> dentro diretório da categoria criada.
	8		Escreve um domínio lido dentro do arquivo <i>domains</i> .
	9		Executa o FP-POS7 até que todos os domínios da lista sejam escritos.
	10		Executa o FP-POS4 ao FP-POS8 até que todas as categorias da lista sejam lidas.
	12		Exibe a mensagem: "A <i>BlackURLLightList-Ativa</i> foi gerada na pasta :[nome da pasta].".
	13		Termina a execução do caso de uso.
	Pós-condições do FP	Código	Descrição/Referência
1		Arquivo gerado com domínios resolvíveis.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Não há.		
Observações	A <i>BlackURLLightList-Ativa</i> será criada em um diretório raiz definido pelo sistema, dentro de uma pasta chamada de Exporta.		

Tabela 15. CDU14 – Gerar BlackURLLightList No Formato BlackList.

5.3.15 Caso de Uso 15 – Gerar BlackURLLightList Reclassificada

Caso de Uso 15 (CDU15)	Gerar <i>BlackURLLightList</i> Reclassificada		
Descrição	Permite gerar um arquivo com domínios resolvíveis no formato da <i>URLBlackList</i> .		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Gerar" e escolhe a opção " <i>BlackURLLightList-Ativa</i> "	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela gerar arquivo <i>BlackURLLightList</i> ativa.
	2	Informa o Nome da pasta e escolhe a opção "Reclassificada".	
	3	Acessa a opção "Gerar".	
	4		Lista as reclassificações realizadas por um administrador.
	5		Lê uma reclassificação
	6		Lista as categorias associadas a uma reclassificação.
	7		Cria uma pasta com o nome da categoria reclassificada dentro de um diretório raiz
	8		Lista os domínios com o status de resolução ativo e que estejam associados a uma categoria da lista de categorias reclassificadas.
	9		Escreve todos os domínio listados dentro do arquivo <i>domains</i> da categoria reclassificada.
	10		Executa o FP-POS-8 a FP-POS-9 até que todas as categorias pertencentes à lista de categorias de uma reclassificação sejam lidas.
	11		Executa o FP-POS-5 a FP-POS-10 até que todas as reclassificações feitas pelo administrador sejam lidas.
	12		Exibe a mensagem: "A <i>BlackURLLightList-Ativa</i> foi gerada na pasta :[nome da pasta].".
	13		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Arquivo gerado com domínios resolvíveis.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Regras de Negócio (RN)	Não há.		
Observações	A <i>BlackURLLightList-Ativa</i> será criada em um diretório raiz definido pelo sistema, dentro de uma pasta chamada de Exporta.		

Tabela 16. CDU15 – Gerar BlackURLLightList Reclassificada.

5.3.16 Caso de Uso 16 – Analisar Arquivo da URLBlackList

Caso de Uso 16 (CDU16)	Analisar Arquivo da <i>URLBlackList</i> .	
Descrição	Permite analisar a resolução dos domínios pertencentes ao arquivo da <i>URLBlackList</i> que ainda não estejam cadastrados, eliminando IP e domínios redundantes e com formatos ilegais (anomalias de resolução). Após a análise de resolução, os domínios são cadastrados com o status atual de resolução. Se um domínio já estiver cadastrado, uma análise de redundância é realizada segundo critérios estabelecidos pelo Administrador. Nesta análise, as categorias encontradas na <i>URLBlackList</i> também são cadastradas.	
Atores	Administrador	
Inclusões	Não há.	
Extensões	Não há.	
Pré-Condições (PRE)	Não há.	
Fluxo Disparador (FD)	Passo	Ator
	1	Acessa o menu "Analisar" e escolhe a opção "Arquivo <i>URLBlackList</i> ".
Fluxo Principal (FP)	Passo	Sistema
	1	Exibe a tela analisar arquivo.
	2	Escolhe um arquivo da <i>URLblackList</i> e a opção "Continuar análise".
	3	Escolhe a opção "Analisar".
	4	Busca uma categoria para reiniciar uma análise.
	5	Registra uma mensagem no <i>log</i> que não existe nenhuma análise de categoria a ser reiniciada.
	6	Lista os nomes das pastas encontradas dentro do diretório da <i>URLBlackList</i> , caso não exista uma análise para reiniciar.
	7	Busca uma categoria com o nome da pasta lido.
	8	Atualiza a categoria em análise para inicializada.
	9	Registra uma mensagem no <i>log</i> que a análise de uma categoria foi inicializada.
	10	Lê um nome do arquivo de domínio da categoria inicializada.
	11	Busca um domínio com o nome lido.
	12	Resolve o domínio, caso ele não seja encontrado.
	13	Registra uma mensagem no <i>log</i> que o domínio foi resolvido.
	14	Lê a resposta de sucesso da resolução.
	15	Interpreta a resposta.
	16	Salva o domínio com os <i>status</i> atual de resolução.
	17	Grava a posição do arquivo em que a leitura do nome de domínio foi feita.
	18	Lê o próximo nome do arquivo de domínio, executando os passos: FP-POS-10 a FP-POS-17 até o fim da leitura do arquivo.
	19	Atualiza a categoria para finalizada.
	20	Registra uma mensagem no <i>log</i> que a análise de uma categoria foi finalizada.
	21	Executa os passos: FP-POS-7 a FP-POS-20 até que todos os nomes da lista de pastas sejam lidos.
	22	Atualiza todas as categorias removendo o status de finalizadas.
	23	Registra uma mensagem no <i>log</i> que a análise do arquivo do <i>URLblackList</i> foi finalizada.
	24	Exibe a seguinte mensagem: "Análise do arquivo finalizada com sucesso".
	25	Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência
	1	Cadastro dos domínios pertencentes à <i>URLBlackList</i> com o <i>status</i> de resolução atual (resolúvel/não resolúvel) e também, o cadastro de todas as categorias existentes.
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 FP	
	Passo	Ator
	1	Acessa a opção "Cancelar".
	2	Exibe a tela inicial do sistema.
	3	Termina a execução do caso de uso.
Fluxo Alternativo 2 (FA2) – "Continuar uma análise"	Ao passo 5 do FP	
	Passo	Ator
	1	Registra uma mensagem no <i>log</i> que a análise foi reiniciada porque uma categoria encontrada.
	2	Lê a última posição acessada do arquivo de

			domínio.
	3		Inicia a leitura do arquivo de domínio da categoria reinicializada na posição lida.
	4		Executa o FP-POS-11 até a posição FP-POS-17.
	5		Retorna a execução do caso de uso para o FP a partir do FP-POS-6 para as categorias que ainda não foram analisadas.
Fluxo Alternativo 3 (FA3) – "Não continuar análise"	Ao passo 2 do FP		
	Passo	Ator	Sistema
	1	Escolhe um arquivo da <i>URLblackList</i> e a opção de não uma "Continuar análise".	
	2	Escolhe a opção "Analisar".	
	3		Busca uma categoria inicializada
	4		Atualiza todas as categorias para não analisadas, caso uma categoria seja encontrada.
	5		Registra uma mensagem no <i>log</i> que a configuração inicial foi restaurada.
	6		Retorna a execução do caso de uso para o FP a partir do FP-POS-6.
Fluxo Alternativo 4 (FA4) – "Categoria não encontrada"	Ao passo 8 do FP		
	Passo	Ator	Sistema
	1		Salva a categoria porque não existe uma categoria com o nome lido.
	2		Retorna a execução do caso de uso para o FP a partir do FP-POS-9.
Fluxo Alternativo 5 (FA5) – "Arquivo de domínio inexistente."	Ao passo 10 do FP		
	Passo	Ator	Sistema
	1		Registra uma mensagem no arquivo de <i>log</i> que o arquivo de domínio de uma categoria não foi encontrado.
	2		Retorna a execução do caso de uso para o FP-POS-19.
Fluxo Alternativo 6 (FA6) – "IP encontrado"	Ao passo 11 do FP		
	Passo	Ator	Sistema
	1		Retorna a execução do caso de uso a partir do FP-POS-17.
Fluxo Alternativo 7 (FA7) – "Domínio encontrado"	Ao passo 12 do FP		
	Passo	Ator	Sistema
	1		Analisa a redundância de domínio segundo o critério estabelecido na [RN1].
	2		Atualiza o domínio, se necessário, para que a [RN1] seja aplicada.
	3		Retorna a execução do caso de uso a partir do FP POS-17.
Fluxo Alternativo 8 (FA8) – "Domínio inicia com hífen"	Ao passo 12 do FP		
	Passo	Ator	Sistema
	1		Resolve domínio com um comando específico porque o nome do domínio inicia com hífen.
	2		Retorna a execução do caso de uso para o FP-POS-13.
Fluxo de Exceção 1 (FE1) – "Diretório inexistente do arquivo"	Ao passo 6 do FP		
	Passo	Ator	Sistema
	1		Interrompe a execução do caso de uso, porque o diretório do arquivo não foi encontrado.
	2		Exibe a seguinte mensagem: "Um erro inesperado ocorreu!".
	3		Termina a execução do caso de uso.
Fluxo de Exceção 2 (FE2) – "Erros de Resolução"	Ao passo 14 do FP		
	Passo	Ator	Sistema
	1		Lê a resposta de erro da resolução.
	2		Identifica um formato inválido de domínio.
	3		Registra uma mensagem no <i>log</i> que o domínio apresentou um erro de resolução.
	4		Retorna a execução do caso de uso para o FP-POS-17.
Fluxo de Exceção 3 (FE3) – "Conectividade inexistente"	Ao passo 2 do FE2		
	Passo	Ator	Sistema
	1		Registra uma mensagem no arquivo de <i>log</i> informando sobre a falha de conectividade.
	2		Interrompe a execução do caso de uso.
	3		Exibe a seguinte mensagem: "Um erro inesperado ocorreu!".
Regras de Negócio (RN)	Código	Descrição	

	1	Em caso de redundância de domínio entre duas ou mais categorias, o domínio deverá ficar associado à categoria que possui o maior grau de perversidade.
Observações		O fluxo principal representa a situação em que usuário escolhe a opção de continuar uma análise, porém não existe nenhuma análise para ser reinicializada.

Tabela 17. CDU16 – Analisar Arquivo da URLBLackList.

5.3.17 Caso de Uso 17 – Analisar Banco de Dados

Caso de Uso 17 (CDU17)	Analisar Banco de Dados.		
Descrição	Permite analisar a resolução dos domínios armazenados, atualizando a <i>status</i> de resolução destes.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Código	Descrição/Referência	
	1	[CDU16-FP-POS1]	
Fluxo Disparador (FD)	Passo	Ator	Sistema
	1	Acessa o menu "Analisar" e escolhe a opção "Banco de Dados."	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela analisar banco de dados.
	2	Escolhe uma das opções de <i>status</i> de domínio para análise: "Ativo", "Inativo" ou "Ambos" e a opção "Continuar análise".	
	3	Escolhe a opção "Analisar".	
	4		Lê o id do último domínio resolvido.
	5		Lista os domínios com o <i>status</i> escolhido e que possuam o id maior que o id lido.
	6		Resolve o domínio lido.
	7		Registra uma mensagem no <i>log</i> que o domínio foi resolvido.
	8		Lê a resposta de sucesso da resolução.
	9		Interpreta a resposta.
	10		Compara a resposta encontrada com a resposta atual.
	11		Atualiza o domínio, caso a resposta seja diferente da atual.
	12		Registra uma mensagem no <i>log</i> que o domínio foi atualizado.
	13		Grava o id do último domínio resolvido.
	14		Retorna a execução do caso de uso a partir do FP-POS-6 ao FP-POS-13 até que toda a lista de domínio seja lida.
	15		Registra uma mensagem no <i>log</i> que a análise do Banco de Dados foi finalizada.
	16		Apaga o id do último domínio lido.
	17		Exibe a seguinte mensagem: "A análise do Banco de Dados foi concluída.".
	18		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Atualização do <i>status</i> de resolução dos domínios armazenados.	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo Alternativo 2 (FA2) – "Não continuar uma análise"	Ao passo 2 do FP		
	Passo	Ator	Sistema
	1	Escolhe uma das opções de <i>status</i> de domínio para análise: "Ativo", "Inativo" ou "Ambos" e a opção de não "Continuar análise".	
	2	Escolhe a opção "Analisar".	
	3		Lista os domínios com o <i>status</i> de domínio escolhido em ordem crescente por id.
	4		Retorna a execução do caso de uso a partir do FP-POS-6.
Fluxo Alternativo 3 (FA3) – "Não existe uma análise para continuar"	Ao passo 5 do FP		
	Passo	Ator	Sistema
	1		Registra uma mensagem no <i>log</i> de que não existe uma análise para reiniciar, caso não exista nenhum id para a leitura.
	2		Retorna a execução do caso de uso a partir do FA2-POS-3.
Fluxo de Exceção 1 (FE1) – "Erros de Resolução"	Ao passo 8 do FP		
	Passo	Ator	Sistema
	1		Lê a resposta de erro da resolução.
	2		Identifica um formato inválido de domínio.

	3		Registra uma mensagem no <i>log</i> que o domínio apresentou um erro de resolução.
	4		Retorna a execução do caso de uso para o FP-POS-13.
Fluxo de Exceção 2 (FE2) – "Conectividade inexistente"	Ao passo 2 do FE1		
	Passo	Ator	Sistema
	1		Registra uma mensagem no arquivo de <i>log</i> informando sobre a falha de conectividade.
	2		Interrompe a execução do caso de uso.
	3		Exibe a seguinte mensagem: "Um erro inesperado ocorreu!".
	4		Termina a execução do caso de uso.
Regras de Negócio (RN)	Não há.		
Observações	Se a opção de status de domínio "Ativo" for escolhida apenas os domínios resolvíveis serão analisados; se a opção "Inativo" for escolhida apenas domínios não resolvíveis serão analisados. Caso a opção "Ambos" for escolhida todos os domínios armazenadas serão analisados.		

Tabela 18. CDU17 – Analisar Banco de Dados.

5.3.18 Caso de Uso 18 – Baixar URLBlackList

Caso de Uso 18 (CDU18)	Baixar <i>URLBlackList</i> .		
Descrição	Realiza o <i>download</i> do arquivo da <i>URLBlackList</i> .		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador 1 (FD1)	Passo	Ator	Sistema
	1	Acessa a opção <i>Download</i> do menu.	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela de <i>download URLBlackList</i> .
	2	Informa a <i>URL</i> do arquivo da <i>URLBlackList</i> .	
	3	Acessa a opção "Baixar".	
	4		Realiza a validação dos dados. [RN1]
	5		Realiza o <i>download</i> do arquivo.
	6		Realiza o <i>download</i> do arquivo MD5 da <i>URLBlackList</i> .
	7		Lê o arquivo MD5.
	8		Escreve o MD5 no arquivo de Configuração <i>XML</i>
	9		Exibe a seguinte mensagem: "O <i>download</i> foi concluído com sucesso.".
	10		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Realiza o <i>download</i> do arquivo da <i>URLBlackList</i> .	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP.		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Código	Descrição	
	1	Todos os campos são obrigatórios.	
Observações	Após o <i>download</i> , o arquivo estará disponível no diretório raiz definido pelo sistema, dentro de uma pasta chamada de <i>Download</i> .		

Tabela 19. CDU18 – Baixar URLBlackList.

5.3.19 Caso de Uso 19 – Verificação URLBlackList

Caso de Uso 19 (CDU19)	Verificar versão <i>URLBlackList</i> .		
Descrição	Verifica se existe uma nova versão da <i>URLBlackList</i> em relação ao último <i>download</i> realizado.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	[CDU18]		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador 1 (FD1)	Passo	Ator	Sistema
	1	Acessa a opção <i>Download</i> do menu.	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela <i>download URLBlackList</i> .
	2	Informa a <i>URL</i> do arquivo MD5 da <i>URLBlackList</i> .	
	3	Acessa a opção "Verificar".	
	4		Realiza a validação dos dados. [RN1]
	5		Realiza o <i>download</i> do arquivo MD5.
	6		Lê o arquivo MD5.
	7		Lê o arquivo de Configuração <i>XML</i> .
	8		Compara o código MD5 dos arquivos lidos.
	9		Exibe a seguinte mensagem: "Existe uma nova versão da <i>URLBlackList</i> disponível para <i>download</i> .", caso os códigos sejam diferentes.
	10		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Informa ao administrador se existe uma nova versão da <i>URLBlackList</i> disponível para <i>download</i> .	
Fluxo Alternativo 1 (FA1) – "Cancelar"	Ao passo 3 do FP.		
	Passo	Ator	Sistema
	1	Acessa a opção "Cancelar".	
	2		Exibe a tela inicial do sistema.
	3		Termina a execução do caso de uso.
Fluxo Alternativo 2 (FA2) – "Não existe nova versão"	Ao passo 9 do FP.		
	Passo	Ator	Sistema
	1		Exibe a seguinte mensagem: "Não existe uma nova versão da <i>URLBlackList</i> disponível para <i>download</i> ".
	2		Termina a execução do caso de uso.
Fluxo Alternativo 2 (FA2) – "Download <i>URLBlackList</i>"	Ao passo 10 do FP		
	Passo	Ator	Sistema
	1	Acessa a opção "Baixar" na tela <i>download URLBlackList</i> .	
	2		Executa o [CDU17]
Fluxo de Exceção (FE)	Nenhum.		
Regras de Negócio (RN)	Código	Descrição	
	1	O campo <i>URL</i> é obrigatório.	
Observações	Não há.		

Tabela 20. CDU19 – Verificar Versão URLBlackList.

5.3.20 Caso de Uso 20 – Efetuar Login

Caso de Uso 20 (CDU20)	Efetuar Login		
Descrição	Permite o acesso aos casos de uso pertencentes ao administrador através de uma autenticação.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Código	Descrição/Referência	
	1	[CDU5-FP-POS1]	
Fluxo Disparador 1 (FD1)	Passo	Ator	Sistema
	1	Acessa a tela principal do usuário.	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela inicial.
	2	Informa o Login e a Senha.	
	3	Escolhe a opção “Entrar”.	
	4		Realiza a validação dos dados. [RN1][RN2]
	5		Permite acesso.
	6		Exibe a tela inicial do sistema para o administrador.
	7		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Acesso ao sistema concedido.	
Fluxo Alternativo (FA)	Não há.		
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Código	Descrição	
	1	Todos os campos são obrigatórios.	
	2	Deve existir um administrador com o login e senha informado.	
Observações	Nenhuma		

Tabela 21. CDU20 – Efetuar Login.

5.3.21 Caso de Uso 21 – Efetuar Logoff

Caso de Uso 21 (CDU21)	Efetuar Logoff		
Descrição	Retira a concessão de acesso ao sistema.		
Atores	Administrador		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Código	Descrição/Referência	
	1	[CDU20-FP-POS1]	
Fluxo Disparador 1 (FD1)	Passo	Ator	Sistema
	1	Acessa a opção "Sair" do menu.	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Retira o acesso do usuário ao sistema.
	2		Exibe a tela inicial do usuário.
	3		Termina a execução do caso de uso.
Pós-condições do FP	Código	Descrição/Referência	
	1	Acesso ao sistema retirado.	
Fluxo Alternativo 1 (FA)	Não há.		
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Nenhum		
Observações	Nenhuma		

Tabela 22. CDU21 – Efetuar Logoff.

5.3.22 Caso de Uso 22 – Download BlackURLLightList

Caso de Uso 22 (CDU22)	<i>Download BlackURLLightList</i>		
Descrição	Permite que um usuário faça o <i>download</i> da <i>BlackURLLightList</i> .		
Atores	Usuário		
Inclusões	Não há.		
Extensões	Não há.		
Pré-Condições (PRE)	Não há.		
Fluxo Disparador 1 (FD1)	Passo	Ator	Sistema
	1	Acessa a opção " <i>Download</i> " da tela principal do usuário.	
Fluxo Principal (FP)	Passo	Ator	Sistema
	1		Exibe a tela <i>Download</i> .
	2	Escolhe o arquivo que deseja baixar.	
	3		O arquivo é fornecido para o <i>download</i> .
	4		Termina a execução do caso de uso.
Pós-condições do FP	Não há.		
Fluxo Alternativo 1 (FA)	Não há.		
Fluxo de Exceção (FE)	Nenhum		
Regras de Negócio (RN)	Nenhum		
Observações	Nenhuma		

Tabela 23. CDU22 – Download BlackURLLightList.

5.4 Diagramas de Classes

O Diagrama de Classes é responsável por modelar aspectos estáticos de um sistema orientados a objetos e é composto de classes e seus relacionamentos. As classes são compostas por atributos e métodos que representam um conjunto de características e comportamento de determinado aspecto do sistema (BEZERRA, 2006).

5.4.1 Diagrama de Classe Conceitual

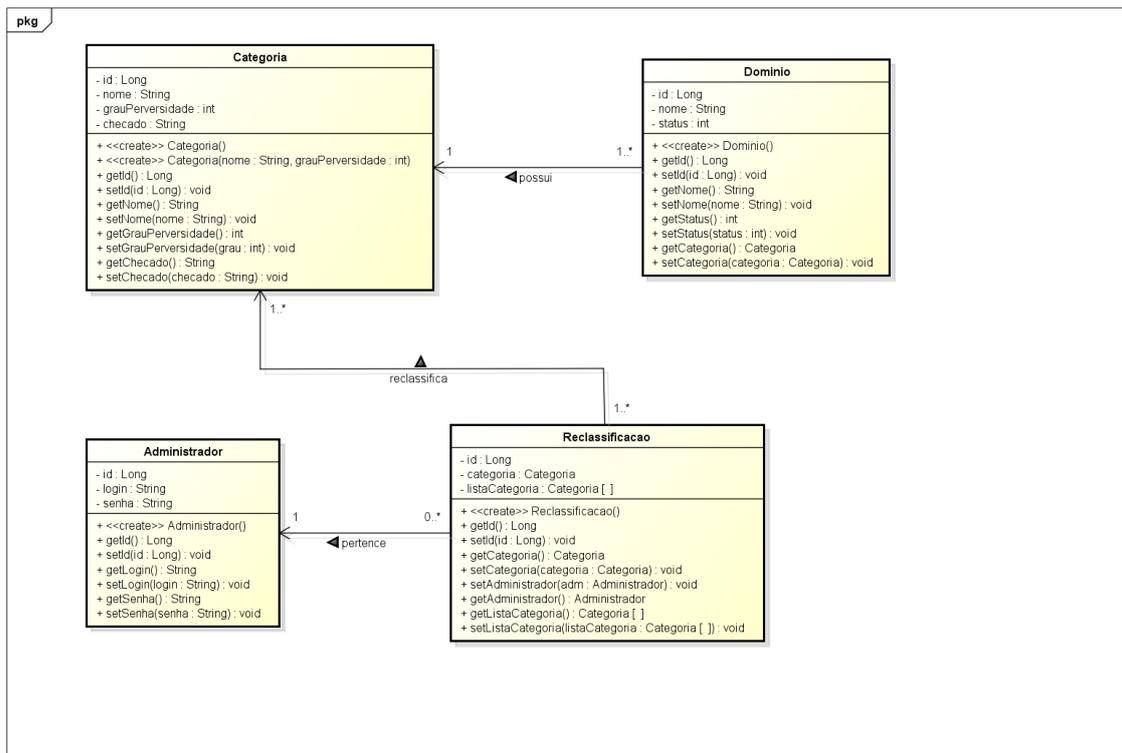


Figura 8. Diagrama de Classe Conceitual.

5.5 Diagramas de Sequência

O Diagrama de Sequência estabelece as interações entre diversos objetos de um sistema de forma temporalmente sequencial. Os objetos têm uma linha de vida e são capazes de trocar mensagens entre si. Este diagrama é responsável por modelar os aspectos dinâmicos de um sistema orientado a objetos (BEZERRA, 2006).

5.5.1 Diagrama de Sequencia – Analisar Banco de Dados

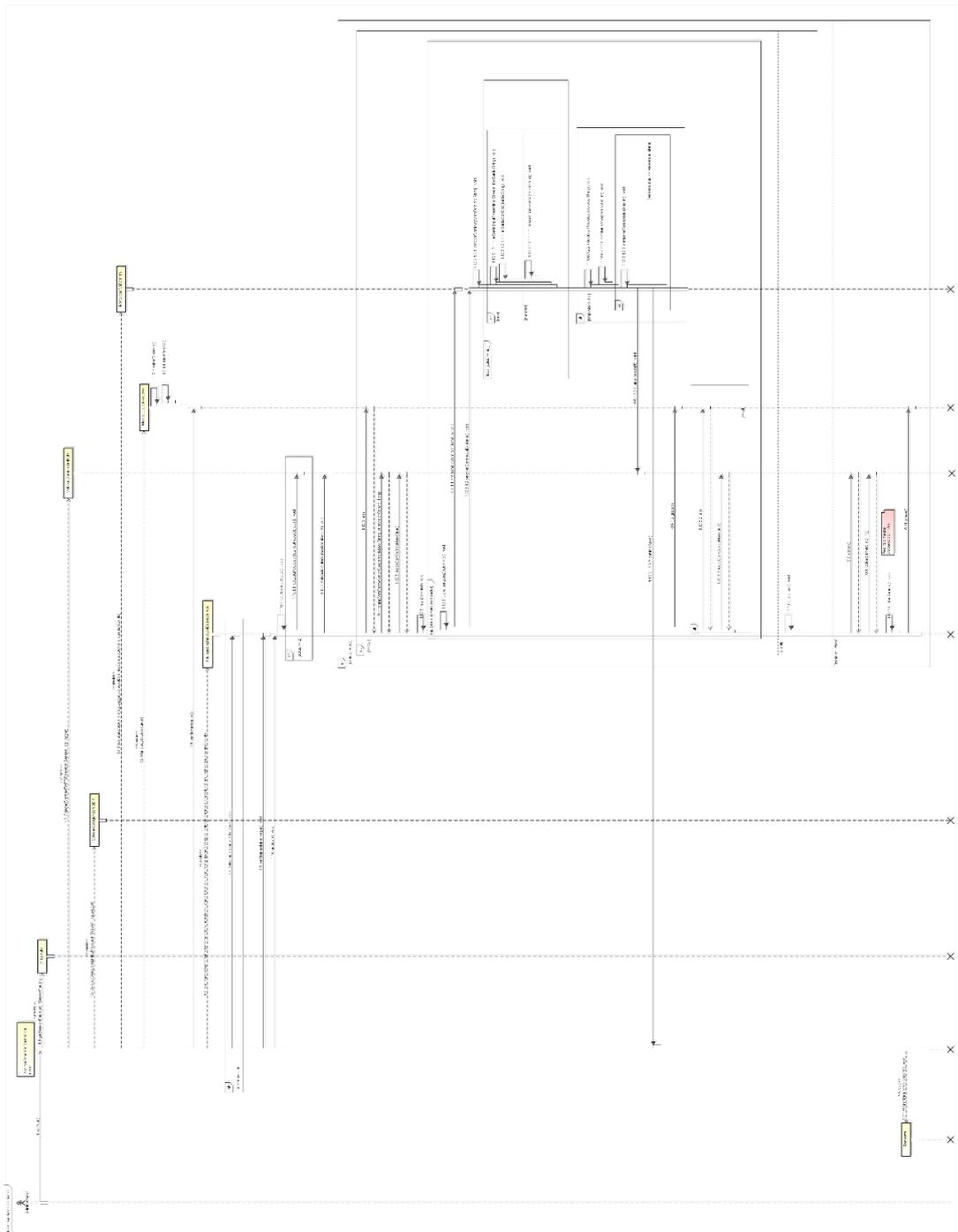


Figura 14. Diagrama de Sequência - Analisar Banco de Dados

5.6 Diagramas de Atividade

O Diagrama de Atividades é um diagrama de interação que tende a observar o comportamento através de diversos casos de uso. O diagrama é utilizado para descrever a lógica algorítmica e processos negócios em passos e é semelhante a um fluxograma (FOWLER, 2005).

5.6.1 Diagrama de Atividade – Analisar Banco de Dados

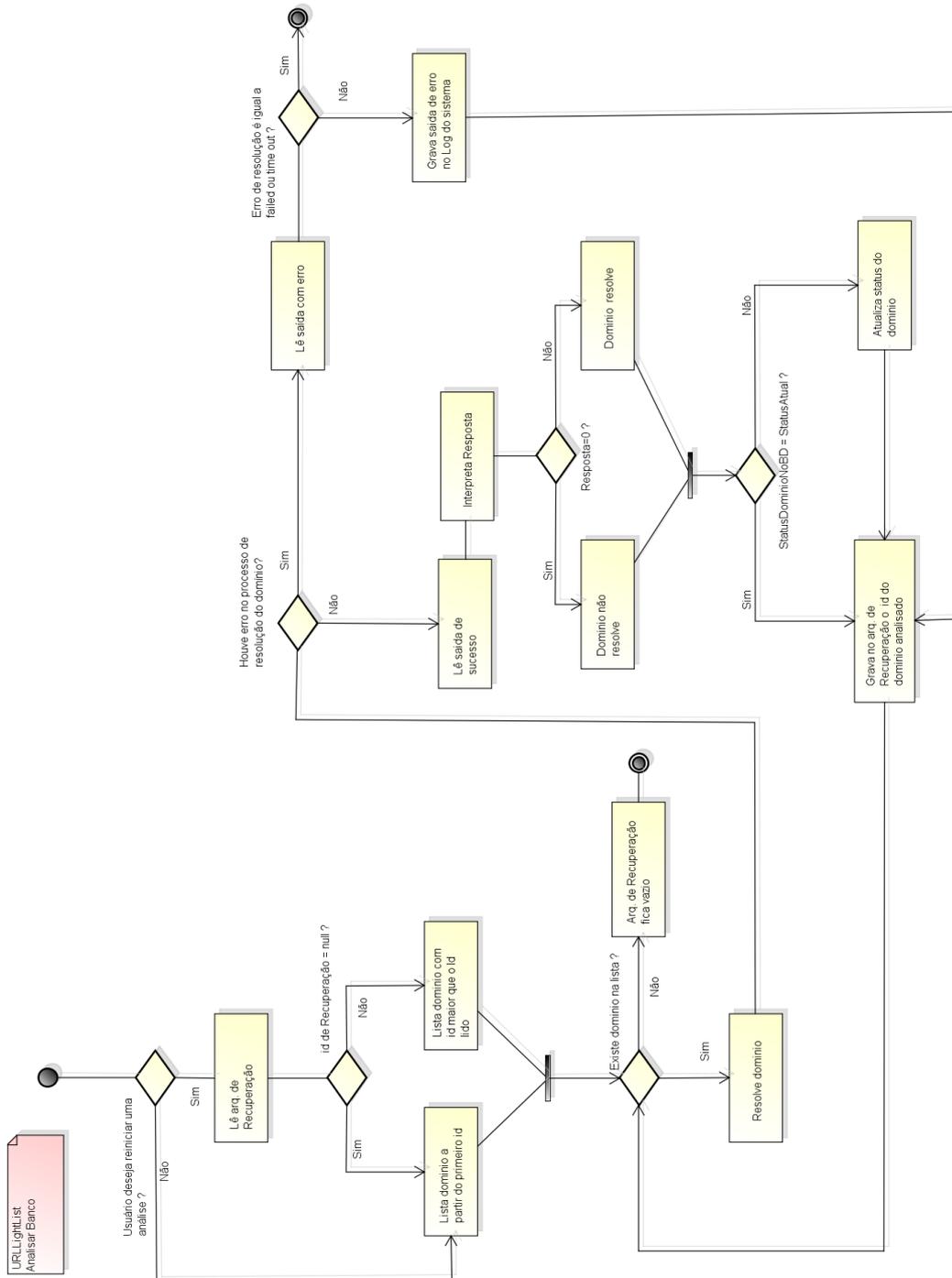


Figura 17. Diagrama de Atividade - Analisar Banco de Dados

5.7 Projeto de Banco de Dados

O projeto de um banco de dados relacional pode ser dividido em três fases distintas: a modelagem conceitual, onde é produzido o Modelo Entidade-Relacionamento (MER), que identifica os principais conceitos de um banco de dados a partir da abstração inicial do negócio; a modelagem lógica, que consiste em montar um modelo mais próximo da lógica da implementação do banco de dados a partir do MER; e a modelagem física, onde, através de uma linguagem de *script* para servidores, o banco de dados é efetivamente criado [HEUSER, 2009]. Neste projeto foi utilizado o MER baseado na notação de Chen (1976) e a ferramenta *GenDBM Tool* [GUINELLI et al., 2015] para design gráfico do MER; e a linguagem de *script* utilizada foi o padrão *ANSI Structured Query Language (SQL)* implementado pelo sistema gerenciador de banco de dados *MySQL*.

A partir do mini-mundo do sistema foi elaborado o MER figura 19 com as entidades *DOMÍNIO*, *CATEGORIA*, *ADMINISTRADOR* e *RECLASSIFICAÇÃO*. Em seguida, este modelo é transformado dando origem ao modelo lógico que identifica com mais detalhes características das entidades, atributos e seus relacionamentos. Por fim, o modelo lógico é transformado em um *script SQL* para ser implementado no *MySQL*. Os modelos lógicos e físicos podem ser encontrados no Anexo IV.

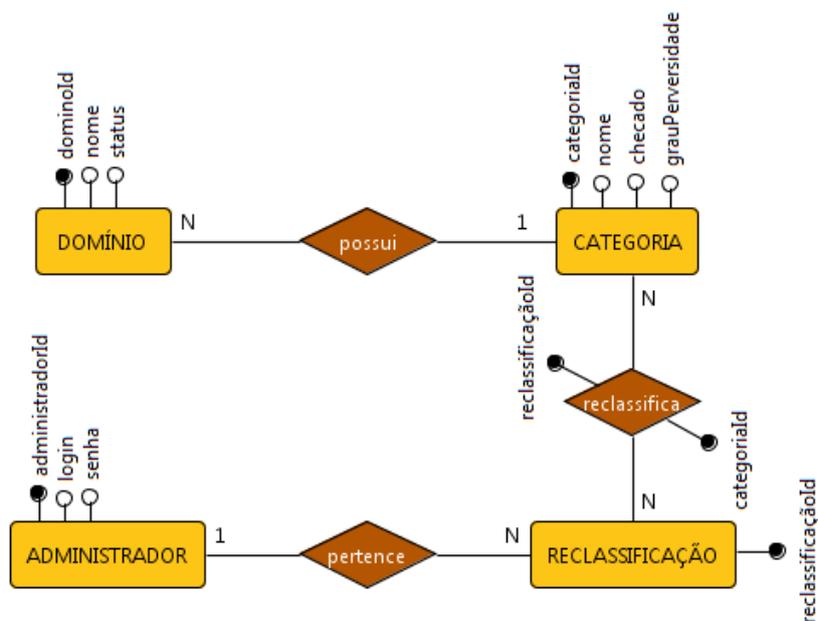


Figura 19. O DER relativo a *BlackURLLightList*.

6 Manual do Sistema

Neste capítulo serão apresentados os manuais de instalação e de utilização da ferramenta *BlackURLLightList*. O manual de instalação conterà os requisitos necessários, bem como as configurações para a instalação da ferramenta tanto para o sistema operacional *Windows* quanto para o sistema operacional *Linux*. E o manual de utilização demonstrará as orientações para executar as principais funcionalidades da ferramenta que são as análises de arquivo e banco de dados e a geração da *BlackURLLightList*.

6.1 Manual de Instalação

Para a instalação da ferramenta *BlackURLLightList* é necessário um servidor que tenha um serviço de hospedagem *web* instalado, como o *Tomcat* da *Fundação Apache* utilizado nesse projeto. Além disso, o servidor deve ter instalado, como sistema de gerenciamento de banco de dados, o *MySQL* e como plataforma para desenvolvimento o *Java Standard Edition (SE)*. Também é necessário que um serviço de resolução de domínio esteja configurado e que os arquivos *JAR* utilizados no projeto sejam colocados na pasta *lib* do servidor *Tomcat* para que não ocorra nenhum erro de compilação. A figura 20 mostra a lista de arquivos *JAR* utilizados no projeto como os *JAR* do *Hibernate* versão 3.0, conector *MySQL*, e o *Log4j*.

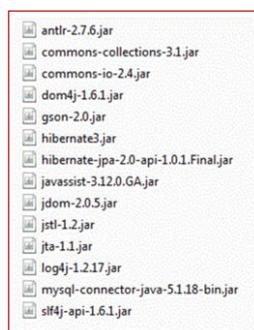


Figura 20. Arquivo *JAR*.

A *BlackURLLightList* foi desenvolvida utilizando a ferramenta de mapeamento objeto relacional *Hibernate*, sendo assim não é necessário a criação manual das tabelas usadas no banco de dados ou importação de um arquivo com as configurações do banco. Os passos necessários são: a criação de um banco de dados com o nome de *BlackURLLightlist*; e de um usuário com nome *tielle* e senha *12345* definido como *localhost*, já que o *Hibernate* criará, automaticamente, todas as tabelas usadas pela ferramenta. Caso o usuário deseje modificar o nome do usuário, do banco e a senha, o arquivo de configuração XML chamado de *hibernate.cfg.xml*, localizado no pacote de denominado *configuracaoHibernate* do projeto, deve ser alterado com as novas informações.

O arquivo de log do projeto *BlackURLLightList* está configurado para ser armazenado na pasta padrão do sistema operacional *Windows*, sendo assim, caso o usuário optar por usar o sistema operacional *Linux* ou optar por usar outro diretório, o arquivo *log4j.properties* do projeto deve ser alterado. Todas as configurações e requisitos necessários para a instalação da ferramenta *URLLightList* tanto no sistema operacional *Linux* quanto *Windows* até o momento são idênticas. Entretanto, para a instalação da *BlackURLLightList* no sistema operacional *Windows* é preciso realizar a instalação do *DIG* usado pela *BlackURLLightList*, já que este comando não está incluído no *Shell* do *Windows*. No *Linux*, a maioria das distribuições já traz esse comando instalado e caso seja preciso instalar, basta o utilizar o gerenciador de pacotes. Para as versões *Debian* e *Ubuntu* de distribuição *Linux*, por exemplo, o comando *apt-get install dnsutils* pode ser usado para a instalação do *DIG*.

6.1.1 Sistema Operacional *Windows*

Para a instalação da ferramenta no sistema operacional *Windows* é necessário que o DIG seja instalado já que o processo de resolução de domínio é realizado por esse comando. Para isso é necessário fazer os seguintes passos:

- Efetuar o *download* do *software* BIND através do *site* oficial (<https://www.isc.org/downloads/>) escolhendo opção para o sistema operacional *Windows* 32 bits ou 64 bits. Nesse projeto a versão do BIND usada foi a versão 9.10.1 - P2;
- Após efetuar o *download*, é preciso descompactar o arquivo e executar o instalador *vcredist.exe*, seguindo a instalação padrão deste;
- Copiar as DLL contidas no diretório raiz do BIND para dentro da pasta *System32* localizada no Disco local (C): dentro da pasta *Windows*, conforme a figura 21:

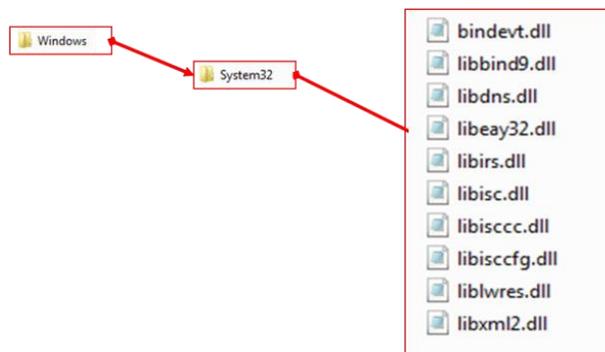


Figura 21. Diretório para instalação DIG.

- Copiar o executável *dig.exe* contido no diretório raiz do BIND também para dentro do diretório *System32*.
- Para testar a instalação, abra o *prompt* de comando e execute DIG.

6.2 Manual de Utilização

O manual de utilização apresentará as orientações para executar as principais funcionalidades da ferramenta *BlackURLLightList* que são: analisar arquivo *URLBlackList*; analisar domínios no banco de dados e gerar *BlackURLLightList* resolvível e não resolvível. A figura 22 ilustra um mapa de navegação a fim de guiar o usuário em relação às opções disponíveis no menu da área administrativa da ferramenta *BlackURLLightList*.

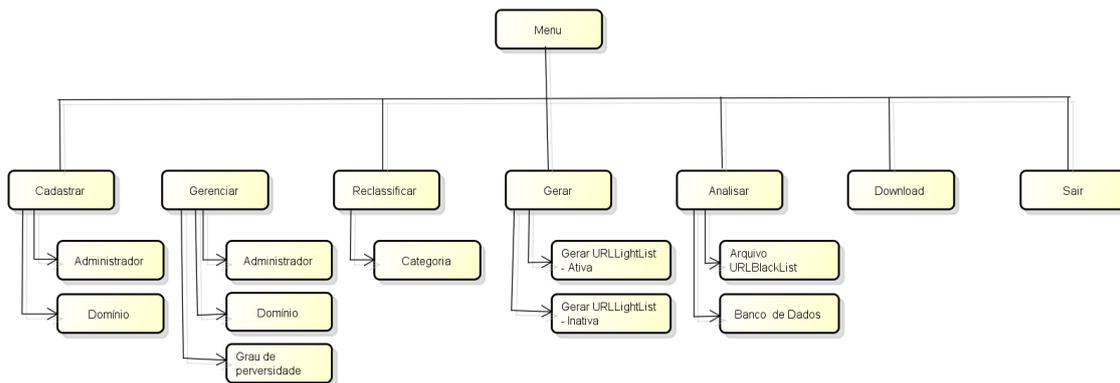


Figura 22. Mapa de navegação.

Na opção cadastrar do menu, o usuário pode cadastrar um domínio e um novo administrador para utilizar a ferramenta; na opção gerenciar o usuário pode atualizar e excluir um domínio e atualizar os dados de um administrador cadastrado. Na opção gerenciar grau de perversidade, os parâmetros (o grau de perversidade) podem ser configurados para o tratamento de redundância dos domínios. A figura 23 mostra a tela de gerenciamento do grau de perversidade, nesta tela o usuário pode atualizar o grau de perversidade de várias categorias de uma só vez. Para isso, deve informar um novo valor de 1 a 10 no campo *Grau de Perversidade* de todas as categorias que deseja atualizar; e depois deve selecionar a opção *Alterar*. Além disso, pode facilmente localizar uma categoria que deseja atualizar através do campo *Search*.

Atualizar Grau de Perversidade

Exibição: 10 registros por página Search:

Nome	Grau de Perversidade
abortion	7 <input type="text"/>
ads	1 <input type="text"/>
adult	8 <input type="text"/>

Exibindo página 1 de 1 First Previous 1 Next Last

Figura 23. Tela de Gerenciamento do Grau de Perversidade.

Na opção reclassificar categoria, o usuário pode unificar várias categorias. Na figura 24, a tela reclassificação de categorias é exibida. O usuário pode escolher um ou quantas categorias desejando, clicando no botão adicionar. O campo nome deve ser informado pelo usuário para nomear a nova categoria a ser criada. Clicando no botão cadastrar a reclassificação de categoria é armazenada. Na listagem de *Categorias aglutinadas*, todas as reclassificações realizadas por um usuário são exibidas possibilitando uma exclusão (ação).

Figura 24. Tela de Reclassificação de Categorias.

Para refinar uma lista da *URLBlackList*, o usuário deve selecionar a opção do menu *Analisar URLBlackList*. Então, o sistema exibe uma tela com todos os arquivos da *URLBlackList* encontrados na pasta chamada de *Download* localizada no diretório raiz. No sistema operacional *Windows*, o diretório raiz possui o caminho *C:/BlackURLLightList/*. Já no *Linux*, o diretório raiz possui o caminho */opt/BlackURLLightList/*. O arquivo da *URLBlackList* a ser escolhido para análise deve estar descompactado e localizado dentro da pasta *Download* do diretório raiz. Após a escolha de um arquivo, basta que o usuário clique no botão *Analisar* e o sistema irá iniciar uma análise. Caso um erro aconteça uma mensagem será exibida na tela. Ao final da análise, uma mensagem também será exibida em caso de sucesso.

Se o campo *Continuar análise* estiver marcado a ferramenta *BlackURLLightList* irá tentar recuperar uma análise que foi interrompida por algum erro no processo, sendo assim, uma análise irá reiniciar de onde parou, analisando apenas as categorias que ainda não foram analisadas. Se não houver uma análise para reiniciar, a ferramenta analisa todas as categorias. Caso o campo o *Continuar análise* não esteja marcado e houver uma análise pendente, a ferramenta irá analisar todas as categorias, mesmo as que já foram analisadas. Todas os eventos importantes do processo de análise são registrados na pasta *log* localizada dentro do diretório raiz. A figura 25 exibe a tela *Analisar Arquivo URLBlackList*.

Figura 25. Tela Analisar Arquivo *URLBlackList*.

Para atualizar o *status* de resolução dos domínios no banco de dados, o usuário deve selecionar a opção do menu *Analisar Banco de Dados*. O usuário deve selecionar qual o tipo de *status* de domínio deseja atualizar. Na opção ativo, somente os domínios resolvíveis serão analisados e atualizados se necessário. Na opção inativo, somente os domínios não resolvíveis serão analisados e atualizados se necessário. Já na opção ambos, domínios resolvíveis e não resolvíveis serão analisados.

Se o campo *Continuar análise* estiver selecionado, a ferramenta irá tentar reiniciar uma análise interrompida por algum erro no processo, sendo assim, apenas domínios ainda não analisados serão submetidos à análise. Se não houver uma análise para reiniciar, a ferramenta irá analisar, normalmente, todos os domínios existentes no banco de dados. E se o campo *Continuar análise* não estiver selecionado, a ferramenta irá analisar todos os domínios existentes no banco de dados, mesmo que houver uma análise pendente.

Para iniciar uma análise, basta o usuário clicar no botão *Analisar* e o sistema irá iniciar uma análise com a opção desejada. Caso um erro aconteça uma mensagem será exibida na tela. Ao final da análise, uma mensagem também será exibida em caso de sucesso. Todos os eventos importantes da análise também será registrado no *log* do sistema. A figura 26 mostra a tela *Analisar Banco de Dados*.



Figura 26. Tela Analisar Banco de Dados.

Para gerar uma lista da *BlackURLLightList* com domínios não resolvíveis, o usuário deve escolher a opção *Gerar BlackURLLightList Inativa*. O sistema irá gerar o arquivo com domínios não resolvíveis em uma pasta chamada de *Exporta* dentro do diretório raiz. Caso um erro aconteça uma mensagem será exibida na tela. Após a geração do arquivo, a ferramenta irá exibir uma mensagem de sucesso.

Para gerar uma lista da *BlackURLLightList* com domínios resolvíveis, o usuário deve escolher a opção *Gerar BlackURLLightList Ativa*. Então, o sistema exibirá uma tela para que o usuário selecione em qual formato deseja gerar a lista da *URLBlackList*. Na opção de formato *URLBlackList*, o sistema irá gerar uma lista de catalogação apenas com os domínios resolvíveis conservando os diretórios da *URLBlackList*. Na opção de formato *Reclassificada*, o sistema irá gerar uma lista de catalogação apenas com os domínios resolvíveis de acordo com reclassificações feitas por um usuário. O usuário deve escolher ainda o nome da pasta que deseja que a lista da *BlackURLLightList* seja gerada. Esta pasta será criada dentro da pasta *Exporta* do diretório raiz. Após fazer essas escolhas o usuário, deve selecionar a opção *Gerar*. Caso um erro aconteça uma mensagem será exibida na tela. Após a geração do arquivo, a ferramenta irá exibir uma mensagem de sucesso. A figura 27 mostra a tela *Gerar BlackURLLightList - Ativa*.

Gerar URLLightList - Ativa

Nome da Pasta:

Tipo de Lista: Formato URLBlackList Reclassificada

Figura 27. Tela Gerar BlackURLLightList - Ativa.

7 Conclusão

Esse projeto apresentou uma ferramenta capaz de realizar um processo de refinamento na lista da *URLBlackList*, segmentando os domínios presentes nessa lista em domínios resolvíveis e não resolvíveis, expurgando IP e domínios com erros de resolução e tratando as redundâncias de domínios quando este pertencer a mais de uma categoria na lista da *URLBlackList*. Após o processo de refinamento, a ferramenta possibilita a geração da *BlackURLLightList*, que é uma lista enxuta composta apenas por domínios resolvíveis, a qual será utilizada por um servidor *Proxy* para realizar um serviço de controle de conteúdo das páginas *web* acessadas por um usuário de uma determinada rede local.

A metodologia empregada no projeto *URLBlackList* foi exposta sendo dividida em três processos principais: o primeiro processo de refinamento explicou em duas etapas como a ferramenta segmenta os domínios existentes na *URLBlackList* e expurga IP ou qualquer domínio que apresente um erro de resolução; o segundo processo foi o de análise de redundância que abordou o tratamento de redundância feito pela ferramenta quando um domínio que pertence a mais de uma categoria na *URLBlackList* for detectado; o último processo abordado foi o processo de reclassificação de categorias que demonstrou como a ferramenta trata as categorias da *URLBlackList* com certas distorções de entendimento quando utilizadas dentro da cultura brasileira.

A implementação mostrou que a ferramenta foi desenvolvida usando o Java EE e o MySQL, como sistema de gerenciamento de banco de dados. Também foi abordado que a ferramenta utilizou o *Hibernate* para realizar o mapeamento objeto relacional entre a ferramenta e o banco de dados. As demais tecnologias empregadas também foram explicadas nesta seção.

Os resultados obtidos pelo processo de refinamento da *URLLightList* revelaram que o processo de refinamento identificou 756.096 domínios não resolvíveis na lista da *URLBlackList* e 942.826 registros foram expurgados por se tratarem de IP, domínios redundantes ou com erros de resolução. O índice redução da *URLBlackList* foi de 58,5 por cento demonstrando que o processo de refinamento proporcionou a geração de uma lista, a *BlackURLLightList*, efetivamente mais enxuta.

Diante do exposto, a ferramenta *BlackURLLightList* conseguiu refinar a lista da *URLBlackList* e atingir o objetivo de gerar uma lista de catalogação com apenas domínios resolvíveis e não redundantes. A lista da *BlackURLLightList* contribui para que recursos computacionais não sejam desperdiçados pelo servidor *Proxy*. Além disso, as categorias da *URLBlackList* agora podem ser adequadas ao contexto brasileiro através do processo de reclassificação proporcionado pela ferramenta.

Como trabalhos futuros, o processo de refinamento poderá ser implementado empregando-se *Threads* para que mais de uma categoria seja analisada ao mesmo tempo, aumentando assim, a performance da ferramenta e diminuindo o tempo gasto em uma análise. Outro fator que poderá melhorar a performance da ferramenta é a conversão do mecanismo de armazenamento do tipo *InnoDB* para *MyISAM*. A simplicidade do mecanismo de armazenamento do tipo *MyISAM* pode proporcionar um maior desempenho nas operações executadas em um banco de dados, melhorando assim, a performance de um *software*. Um novo experimento poderá ser realizado utilizando o mecanismo de armazenamento do tipo *MyISAM* para que seja possível comprovar o aumento de performance da ferramenta em um processo de refinamento.

Ao processo de analisar banco de dados e arquivo, um botão de parada deverá ser disponibilizado para que o usuário possa interromper o processo de análise quando desejar. Um processo que possibilite que um usuário carregue todas as categorias do arquivo da *URLBlackList*, antes de uma análise, cadastrando as categorias com o grau de perversidade que desejar poderá ser implementado. Também poderá ser implementado uma funcionalidade de

agendamento para que a ferramenta dispare uma análise de banco de dados, automaticamente e um aperfeiçoamento do tratamento de erro do *time out*.

Anexo I – Categorias da URLBlackList

Tabela Categorias URLBlackList			
	Categoria		
		48	hygiene
1	abortion	49	instantmessaging
2	ads	50	jewelry
3	adult	51	jobsearch
4	aggressive	52	kidstimestwasting
5	alcohol	53	lingerie
6	antispyware	54	magazines
7	arjel	55	mail
8	artnudes	56	malware
9	astrology	57	manga
10	audio-video	58	marketingware
11	bank	59	medical
12	banking	60	mixed_adult
13	beerliquorinfo	61	mobile-phone
14	beerliquorsale	62	naturism
15	bitcoin	63	news
16	blog	64	onlineauctions
17	books	65	onlinegames
18	celebrity	66	onlinepayment
19	cellphones	67	personalfinance
20	chat	68	pets
21	child	69	phishing
22	childcare	70	porn
23	cleaning	71	press
24	clothing	72	proxy
25	contraception	73	radio
26	cooking	74	reaaffected
27	culinary	75	religion
28	dating	76	remote-control
29	desktopsillies	77	ringtones
30	dialers	78	searchengines
31	drugs	79	sect
32	ecommerce	80	sexuality
33	educational_games	81	sexualityeducation
34	entertainment	82	shopping
35	filehosting	83	social_networks
36	filesharing	84	socialnetworking
37	financial	85	sportnews
38	frencheducation	86	sports
39	gambling	87	spyware
40	games	88	tobacco
41	gardening	89	translation
42	government	90	updatesites
43	guns	91	vacation
44	hacking	92	verisign
45	homerepair	93	violence
46	humor	94	virusinfected
47	hunting	95	warez
		96	weapons
		97	weather
		98	webmail
		99	whitelist

Anexo II - Tabelas de Resultado Obtido por Categoria

Tabela de Resultado Obtido por Categoria						
Categoria	URLBlackList	URLLightList Resolvível	URLLightList Não Resolvível	Domínios com formato ilegais/redundantes/IP	índice redução (%)	
1	abortion	736	682	52	2	7%
2	ads	28.766	13.307	5.862	9.597	54%
3	adult	997.238	272.664	195.824	528.750	73%
4	aggressive	433	105	19	309	76%
5	alcohol	11.028	10.115	873	40	8%
6	antispyware	35	25	5	5	29%
7	arjel	69	7	4	58	90%
8	artnudes	69	44	8	17	36%
9	astrology	29	24	1	4	17%
10	audio-video	3.800	2.489	475	836	35%
11	bank	1.696	1.598	97	1	6%
12	banking	2.841	1.279	317	1.245	55%
13	beerliquorinfo	8	5	1	2	38%
14	beerliquorsale	2	2	-	0	0%
15	bitcoin	249	166	58	25	33%
16	blog	1.469	1.228	175	66	16%
17	books	8.013	6.976	875	162	13%
18	celebrity	625	390	76	159	38%
19	cellphones	46	33	8	5	28%
20	chat	806	419	100	287	48%
21	child	38	24	2	12	37%
22	childcare	45	43	2	0	4%
23	cleaning	178	55	14	109	69%
24	clothing	172	157	12	3	9%
25	contraception	127	74	5	48	42%
26	cooking	16	15	1	0	6%
27	culinary	26	23	2	1	12%
28	dating	3.796	2.611	883	302	31%
29	desktopsillies	1.260	1.021	197	42	19%
30	dialers	33	13	4	16	61%
31	drugs	1.046	383	73	590	63%

	Categoria	URLBlackList	URLLightList Resolúvel	URLLightList No Resolúvel	Domínios com formato ilegais/redundantes/IP	índice redução (%)
32	ecommerce	142.049	109.755	24.023	8.271	23%
33	educational_games	7	3	-	4	57%
34	entertainment	210	127	27	56	40%
35	filehosting	834	540	119	175	35%
36	filesharing	186	152	15	19	18%
37	financial	77	49	16	12	36%
38	frencheducation	1.002	671	254	77	33%
39	gambling	5.487	4.373	1.014	100	20%
40	games	9.532	8.046	1.259	227	16%
41	gardening	46	43	3	0	7%
42	government	499	266	222	11	47%
43	guns	2.406	2.179	227	0	9%
44	hacking	581	90	25	466	85%
45	homerepair	21	7	9	5	67%
46	humor	5.864	4.750	680	434	19%
47	hunting	5.061	4.542	464	55	10%
48	hygiene	15	12	3	0	20%
49	instantmessaging	179	90	18	71	50%
50	jewelry	5	2	2	1	60%
51	jobsearch	2.016	1.801	211	4	11%
52	kidstimestwasting	1.638	831	157	650	49%
53	lingerie	27	21	2	4	22%
54	magazines	7.647	5.561	550	1.536	27%
55	mail	2.691	1.523	1.027	141	43%
56	malware	340.030	25.633	53.176	261.221	92%
57	manga	537	422	68	47	21%
58	marketingware	191	111	35	45	42%
59	medical	117.381	90.495	15.272	11.614	23%

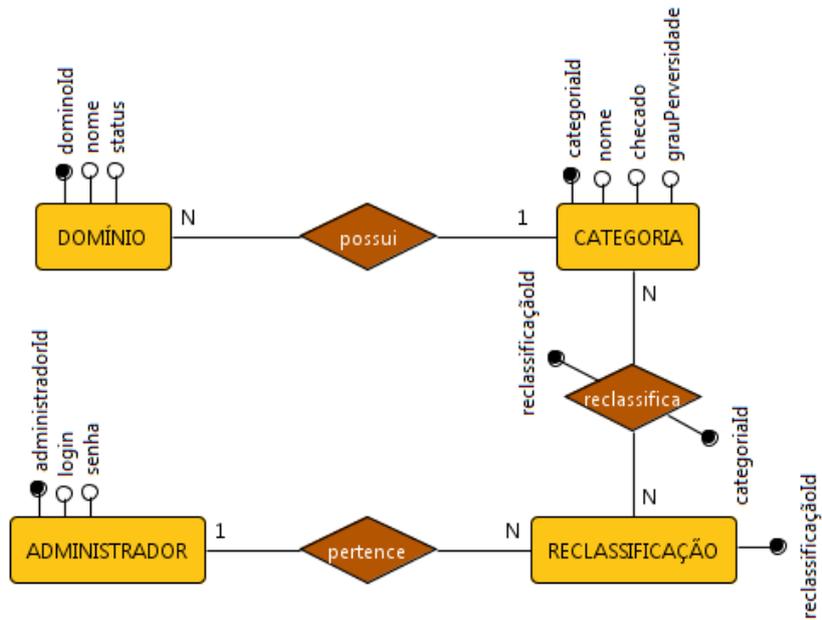
Categoria		URLBlackList	URLLightList Resolvível	URLLightList Não Resolvível	Domínios com formato ilegais/redundantes/IP	índice redução (%)
60	mixed_adult	137	71	15	51	48%
61	mobile-phone	45	35	6	4	22%
62	naturism	62	38	5	19	39%
63	news	7.446	6.684	546	216	10%
64	onlineauctions	67	54	10	3	19%
65	onlinegames	1.402	577	170	655	59%
66	onlinepayment	43	26	12	5	40%
67	personalfinance	75	51	13	11	32%
68	pets	26.911	17.615	4.887	4.409	35%
69	phishing	121.388	18.711	82.098	20.579	85%
70	porn	527.846	230.013	245.597	52.236	56%
71	press	4.446	2.670	69	1.707	40%
72	proxy	107.118	43.026	57.579	6.513	60%
73	radio	625	538	59	28	14%
74	reaffected	8	3	3	2	63%
75	religion	110.333	92.577	16.409	1.347	16%
76	remote-control	41	36	2	3	12%
77	ringtones	61	35	21	5	43%
78	searchengines	212	178	16	18	16%
79	sect	145	123	18	4	15%
80	sexuality	276	246	8	22	11%
81	sexualityeducation	46	34	1	11	26%
82	shopping	36.382	13.951	805	21.626	62%
83	social_networks	636	482	40	114	24%
84	socialnetworking	376	258	66	52	31%
85	sportnews	89	79	8	2	11%
86	sports	89.421	71.664	17.445	312	20%
87	spyware	193	49	45	99	75%
88	tobacco	675	608	65	2	10%

Categoria	URLBlackList	URLLightList Resolvível	URLLightList Não Resolvível	Domínios com formato ilegais/redundantes/IP	índice redução (%)
89 translation	167	166	-	1	1%
90 updatesites	13	9	2	2	31%
91 vacation	151.146	122.231	24.619	4.296	19%
92 verisign	2	0	2	0	100%
93 violence	63	24	6	33	62%
94 virusinfected	341	201	124	16	41%
95 warez	1.228	596	309	323	51%
96 weapons	111	81	14	16	27%
97 weather	165	154	10	1	7%
98 webmail	618	412	68	138	33%
99 whitelist	101	74	21	6	27%

Anexo III – Tabela de Grau de Perversidade

Tabela Grau de Perversidade					
Categoria	Grau	Categoria	Grau	Categoria	Grau
vacation	1	magazines	1	press	1
bank	1	child	1	malware	10
games	10	culinary	1	remote-control	1
sportnews	1	arjel	1	beerliquorinfo	3
spyware	10	reaaffected	1	medical	1
manga	1	porn	10		
social_networks	5	sect	3		
onlineauctions	3	webmail	1		
bitcoin	1	beerliquorsale	3		
whitelist	1	astrology	1		
gambling	10	onlinegames	10		
pets	1	cellphones	1		
translation	1	childcare	1		
chat	5	hunting	1		
blog	3	antispysware	1		
desktopsillies	8	gardening	1		
audio-video	1	homerepair	1		
frencheducation	1	kidstimestwasting	1		
radio	6	virusinfected	10		
guns	10	personalfinance	1		
educational_games	2	updatesites	1		
searchengines	1	dialers	10		
news	1	government	1		
filehosting	1	weapons	10		
onlinepayment	1	weather	1		
phishing	10	hygiene	1		
entertainment	1	banking	1		
clothing	1	religion	1		
mixed_adult	3	naturism	5		
ringtones	2	marketingware	1		
sports	1	cooking	1		
humor	1	shopping	1		
celebrity	1	violence	8		
sexuality	9	tobacco	1		
artnudes	5	verisign	1		
books	1	dating	8		
sexualityeducation	1	adult	9		
drugs	10	socialnetworking	5		
filesharing	1	mobile-phone	1		
aggressive	6	proxy	10		
instantmessaging	10	contraception	1		
jewelry	1	warez	10		
jobsearch	1	lingerie	5		
mail	1	alcohol	5		
ecommerce	1	ads	1		
hacking	10	abortion	10		
financial	1	cleaning	1		

Anexo IV – Modelo Lógico e Modelo Físico do Banco de Dados



DOMÍNIO(dominioId, nome, status, categoriaId)

categoriaId REFERENCIA CATEGORIA

CATEGORIA(categoriaId, nome, checado, grauPerversidade)

ADMINISTRADOR(administradorId, login, senha)

RECLASSIFICAÇÃO(reclassificacaoId, administradorId)

administradorId REFERENCIA ADMINISTRADOR

RECLASSIFICA(reclassificacaoId, categoriaId)

reclassificacaoId REFERENCIA RECLASSIFICACAO

categoriaId REFERENCIA CATEGORIA

```
-- phpMyAdmin SQL Dump
-- version 4.1.14
-- http://www.phpmyadmin.net
--
-- Host: 127.0.0.1
-- Generation Time: 19-Jun-2015 Ã s 07:32
-- VersÃo do servidor: 5.6.17
-- PHP Version: 5.5.12

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT
*/;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS
*/;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION
*/;
/*!40101 SET NAMES utf8 */;

--
-- Database: `urllightlist`
--

-----

--
-- Estrutura da tabela `administrador`
--

CREATE TABLE IF NOT EXISTS `administrador` (
  `administrador_id` bigint(20) NOT NULL AUTO_INCREMENT,
  `login` varchar(255) NOT NULL,
  `senha` varchar(255) NOT NULL,
  PRIMARY KEY (`administrador_id`),
  UNIQUE KEY `login` (`login`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=12 ;

-----

--
-- Estrutura da tabela `categoria`
--

CREATE TABLE IF NOT EXISTS `categoria` (
  `categoria_id` bigint(20) NOT NULL AUTO_INCREMENT,
  `checado` varchar(255) DEFAULT NULL,
  `grauPerversidade` int(11) NOT NULL,
  `nome` varchar(255) NOT NULL,
  PRIMARY KEY (`categoria_id`),
  UNIQUE KEY `nome` (`nome`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=71 ;
```

```

-----

--
-- Estrutura da tabela `dominio`
--

CREATE TABLE IF NOT EXISTS `dominio` (
  `dominio_id` bigint(20) NOT NULL AUTO_INCREMENT,
  `nome` varchar(255) NOT NULL,
  `status` int(11) NOT NULL,
  `categoria_id` bigint(20) NOT NULL,
  PRIMARY KEY (`dominio_id`),
  UNIQUE KEY `nome` (`nome`),
  KEY `FK6D8A794D86AE7F51` (`categoria_id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=187 ;

-----

--
-- Estrutura da tabela `reclassificacao_categoria`
--

CREATE TABLE IF NOT EXISTS `reclassificacao_categoria` (
  `reclassificacao_id` bigint(20) NOT NULL,
  `categoria_id` bigint(20) NOT NULL,
  KEY `FK306F0FC2FCEC7371` (`reclassificacao_id`),
  KEY `FK306F0FC286AE7F51` (`categoria_id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-----

--
-- Estrutura da tabela `reclassificacao`
--

CREATE TABLE IF NOT EXISTS `reclassificacao` (
  `reclassificacao_id` bigint(20) NOT NULL AUTO_INCREMENT,
  `administrador_id` bigint(20) NOT NULL,
  `categoria_id` bigint(20) NOT NULL,
  PRIMARY KEY (`reclassificacao_id`),
  KEY `FKC61B196C93D7F956` (`categoria_id`),
  KEY `FKC61B196C956FF716` (`administrador_id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=12 ;

--
-- Constraints for dumped tables
--

--
-- Limitadores para a tabela `dominio`
--
ALTER TABLE `dominio`
  ADD CONSTRAINT `FK6D8A794D86AE7F51` FOREIGN KEY
  (`categoria_id`) REFERENCES `categoria` (`categoria_id`);

```

```

--
-- Limitadores para a tabela `reclassificacao_categoria`
--
ALTER TABLE `reclassificacao_categoria`
  ADD CONSTRAINT `FK306F0FC286AE7F51` FOREIGN KEY
(`categoria_id`) REFERENCES `categoria` (`categoria_id`),
  ADD CONSTRAINT `FK306F0FC2FCEC7371` FOREIGN KEY
(`reclassificacao_id`) REFERENCES `reclassificacao`
(`reclassificacao_id`);

--
-- Limitadores para a tabela `reclassificacao`
--
ALTER TABLE `reclassificacao`
  ADD CONSTRAINT `FKC61B196C93D7F956` FOREIGN KEY
(`categoria_id`) REFERENCES `categoria` (`categoria_id`),
  ADD CONSTRAINT `FKC61B196C956FF716` FOREIGN KEY
(`administrador_id`) REFERENCES `administrador`
(`administrador_id`);

/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS
*/;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;

```

8 Referências Bibliográficas

BEZERRA, Eduardo. **Princípios de Análise e Projetos de Sistemas com UML** – Rio de Janeiro: Elsevier, 2006.

BIND. **BIND**. Disponível em: < <https://www.isc.org/downloads/bind/>>. Acesso em: 12 de junho de 2015.

COUTINHO, F. **Vantagens e Desvantagens Das Redes Sociais - Comunicação e Interesses | Tecnologia - Cultura Mix**. Disponível em: <<http://tecnologia.culturamix.com/internet/vantagens-e-desvantagens-das-redes-sociais>>. Acesso em: 12 de abril de 2012.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores** – Porto Alegre: Bookman, 2008.

FOWLER, Martin. KOBRYN, Cris. **UML Essencial** – Porto Alegre: Bookman, 2005.

GOOGLEPUBLICDNS. **GooglePublicDNS**. Disponível em: <<https://developers.google.com/speed/public-dns/>>. Acesso em: 12 de junho de 2015.

GUINELLI, J. V., ROSA, A. S., PANTOJA, C. E., CHOREN, R. **Uma Metodologia para Apoio ao Projeto de Banco de Dados Geográficos Utilizando a MDA**. In **X Simpósio Brasileiro de Sistemas de Informação**. 2014. Sociedade Brasileira de Computação.

HEUSER, C. A. **Projeto de Banco de Dados**. 6ed. Bookman, 2009.

IBOPE. **94,2 milhões de pessoas tem acesso à internet no Brasil**. Disponível em: <<http://www.ibope.com.br/pt-br/relacionamento/imprensa/releases/Paginas/942-milhoes-de-pessoas-tem-acesso-a-internet-no-Brasil.aspx>>. Acesso em: 10 de abril de 2013.

KRASNER, G. E., POPE, S. T. *A description of the Model-View-Controller user interface paradigm in the Smalltalk-80 System*. 1988. Disponível em: www.create.ucsb.edu/~stp/PostScript/mvc.pdf. Acesso em: 05 de julho de 2015.

MORIMOTO, Carlos Eduardo. **Servidores Linux, guia prático** – Porto Alegre: Sul Editores, 2009.

OPENDNS. **OpenDNS**. Disponível em: <<https://www.opendns.com/>>. Acesso em: 12 de junho de 2015.

URLBLACKLIST. **UrlBlackList**. Disponível em: <<http://urlblacklist.com/?sec=search>>. Acesso em: 12 de junho de 2015.

WAZLAWICK, Raul Sidnei. **Metodologia de pesquisa para ciência da computação** – Rio de Janeiro: Elsevier, 2008.