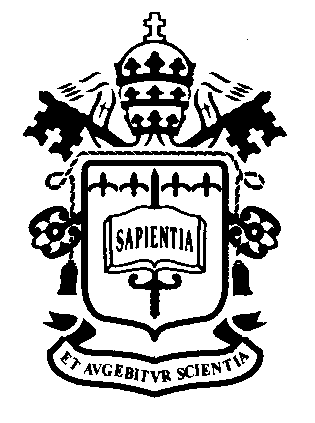
**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO**

**CURSO DE ESPECIALIZAÇÃO EM ENGENHARIA DE SOFTWARE**

**PAULO VITOR DA SILVA RENDEIRO**

**COMUNICAÇÃO AJAX CROSS-DOMAIN UTILIZANDO O MECANISMO CROSS-ORIGIN RESOURCE SHARING**

SÃO PAULO, SETEMBRO DE 2011

**PAULO VITOR DA SILVA RENDEIRO**

**COMUNICAÇÃO AJAX CROSS-DOMAIN UTILIZANDO O MECANISMO CROSS-ORIGIN RESOURCE SHARING**

Monografia apresentada ao Curso de Especialização em Engenharia de Software da Pontifícia Universidade Católica de São Paulo, como requisito parcial para obtenção do título de Especialista em Engenharia de Software, orientado pelo Prof. Dr. Carlos Eduardo de Barros Paes.

SÃO PAULO, SETEMBRO DE 2011

**COMUNICAÇÃO AJAX CROSS-DOMAIN UTILIZANDO O MECANISMO CROSS-ORIGIN RESOURCE SHARING**

**PAULO VITOR DA SILVA RENDEIRO**

Monografia defendida e aprovada, em (*data da defesa*), pela banca examinadora:

Professor Doutor Carlos Eduardo de Barros Paes

Orientador

Professor Mestre (Nome do Primeiro Avaliador)

Professor do curso de...

Professor Especialista (Nome do Segundo Avaliador)

Professor do curso de...

**Dedico** este trabalho a todos aqueles que contribuíram de forma direta ou indireta para conclusão do mesmo.

Agradeço primeiramente a Deus...

"O analfabeto do século XXI não será aquele que não sabe ler e escrever, mas aquele que não consegue aprender, desaprender e aprender novamente"

Alvin Tofler

LISTA DE FIGURAS

Listagem dos títulos de todas as figuras apresentadas no texto seguido dos números das páginas. Sugere-se que esta indicação seja construída de forma automática usando recursos do próprio editor de texto (formatar cada título de figura com um estilo específico, por exemplo FIGURA e após inserir índice).

[**Figura 1. Exemplo de uma figura no texto. (RIBEIRO, 2006) 19**](#_Toc178715233)

LISTA DE TABELAS

Listagem dos títulos de todas as tabelas apresentadas no texto seguido dos números das páginas. Sugere-se que esta indicação seja construída de forma automática usando recursos do próprio editor de texto (formatar cada título de tabela com um estilo específico, por exemplo TABELA e após inserir índice).

[**Tabela 1 – Tabela de formatos para monografia 20**](#_Toc178715289)

RESUMO

O resumo não apresenta recuos e parágrafos, portanto trata-se de um texto corrido que aborda as principais partes de um trabalho científico: introdução (objeto de estudo, problema, tema, área e sub-área), objetivos (geral e específicos), justificativas, metodologia, resultados esperados ou finais e conclusões. Este resumo deve conter de 200 a 400 palavras de forma a indicar as idéias principais apresentadas no texto. O resumo não deve ser confundido com uma introdução do trabalho e muito menos conter abreviações, referências bibliográficas, figuras, etc. Na elaboração deste resumo, como também em todo o trabalho, deve ser utilizada a forma impessoal como, por exemplo, “... Os resultados experimentais mostraram que...” ao invés de “...os resultados que nós obtivemos mostraram que...”. Deve indicar os principais pontos do trabalho: objeto de estudo, problema, tema, objetivos, metodologia, resultados esperados ou obtidos, o valor científico do trabalho e sua originalidade. Deve ser seguido das palavras-chave, isto é, das palavras que mais representam o conteúdo do trabalho.

**Palavras-chave:** Os autores devem apresentar um conjunto de no máximo 3 palavras-chave (em ordem alfabética) que possam identificar os principais tópicos abordados no trabalho.

ABSTRACT

O texto do abstract é o mesmo contido no resumo porém escrito na língua inglesa.

**Keywords**: palavras-chaves escrito na língua inglesa.

SUMÁRIO

1.1 Contextualização 11

1.2 Problema 12

1.3 Problematização 12

1.4 Objetivos 13

1.4.1 Objetivos gerais 13

1.4.2 Objetivos específicos 13

1.5 Relevância 14

1.6 Introdução 18

1.7 Referencial Teórico 18

1.7.1 Subseções 19

1.8 Figuras 19

1.9 Tabelas 20

2.1 Introdução 22

2.2 Conclusões 22

2.3 Trabalhos Futuros 22

# INTRODUÇÃO

## Contextualização

Com o crescimento e a popularização de APIs para o desenvolvimento de aplicações baseadas em Asynchronous Javascript and XML (AJAX), como jQuery, Prototype e ExtJS, é cada vez maior o número de aplicações que combinam dados e códigos provenientes de diversas fontes espalhadas pela internet, proporcionando a criação de inúmeros novos serviços e funcionalidades.

Quando este tipo de aplicação é desenvolvido, encontram-se diversas dificuldades inerentes a realização de comunicações AJAX com serviços de outras origens. Nesta contexto, uma origem é definida pela combinação de um protocolo, um domínio e uma porta [FLANAGAN, 2011].

O principal obstáculo na execução de uma chamada AJAX Cross-Domain é o conceito de segurança Same-Origin Policy (SOP), introduzido pelo navegador Netscape 2.0 em Março de 1996 [PRATES, 2010]. Este conceito de segurança é aplicado a linguagens de programação que são executadas no navegador, como JavaScript, e limita o acesso à maioria das propriedades entre páginas de domínios diferentes, como funções JavaScript, cookies e dados de formulários. Tais restrições foram criadas para mitigar ataques de Cross-site scripting (XSS) e Cross-site request forgery (CSRF/XSRF) [FLANAGAN, 2011].

A política de mesma origem, devido a sua característica de forte restrição, maximizou consideravelmente a segurança dos navegadores e é adotada em todos os navegadores web modernos. Porém, a comunicação AJAX entre origens distintas não é por natureza insegura ou mal, é de fato essencial para muitas das aplicações mais populares e utilizadas do mundo [JSON-P, 2008].

Diante da emergente necessidade da troca de informações entre aplicações de diferentes origens via AJAX, foram desenvolvidos diversos mecanismos para contornar as limitações impostas pelo SOP. Alguns dos mais conhecidos são:

1. Equiparação de domínio: este método iguala os domínios das aplicações através da propriedade “document.domain”, permitindo assim a execução de requisições AJAX. Esta técnica, porém, só funciona para cenários de cross-subdomain.
2. Cross-Origin Messaging: especificada pelo HTML 5, essa é uma nova forma de comunicação assíncrona entre janelas do navegador, inclusive para documentos carregados em iframes. Sua utilização se dá pela invocação da função “window.postMessage”. Pela sua finalidade, entretanto, esta técnica não prevê suporte para comunicação AJAX.
3. Server-side proxy: consiste em efetuar as chamadas AJAX para uma URL da sua própria aplicação e, no lado servidor, fazer a chamada para o serviço cross-domain. Este mecanismo atende ao cenário de cross-domain para requisições que utilizem os mais variados verbos HTTP, porém sua implementação, além de intrusiva, demanda muito esforço de configuração e aumenta a complexidade de implantação da aplicação.
4. JavaScript Object Notation with Padding (JSONP): esta técnica utiliza a simples técnica do servidor retornar um código Javascript que passa um JSON para uma função de callback provida pelo lado cliente via parâmetro da requisição. Este método funciona para cenários cross-domain, porém apenas com requisições que utilizam GET como verbo HTTP, além de não ser aderente ao modelo de comunicação AJAX.

## Problema

Atualmente para implementarmos um diálogo cross-domain via AJAX temos poucas alternativas técnicas disponíveis, sendo que estas possuem muitas limitações de segurança e contra-indicações. A falta de um modelo robusto e padronizado de comunicação entre origens dissemelhantes gera uma lacuna que muitas vezes é preenchida por soluções inseguras e muito complexas, que acabam, respectivamente, expondo dados sensíveis e degradando a manutenabilidade da aplicação.

## Problematização

Com o contexto mencionado, questiona-se:

1. Como abstrair a complexidade no desenvolvimento de sistemas que necessitem consumir, através de requisições AJAX, serviços expostos em diversos domínios?
2. Como expor serviços na internet que possam ser consumidos apenas por origens autorizadas?
3. Como fazer o controle do nível de acesso de acordo com o recurso solicitado e origem da requisição?
4. Como estender a API de chamadas AJAX, disponibilizada pelos navegadores web, para saber trabalhar requisições cross-domain mantendo sua interface original?
5. Como tornar possível o uso dos mais variados verbos HTTP, como: GET, POST, PUT, DELETE e OPTIONS, na realização de requisições AJAX cross-domain?

## Objetivos

### Objetivos gerais

O objetivo deste projeto é apresentar a especificação Cross-Origin Resource Sharing (CORS), desenvolvida pelo pelo consórcio W3C para o compartilhamento de recursos consumíveis por aplicações de outros domínios através de chamadas AJAX, estendendo o conceito de segurança Same-Origin Policy.

### Objetivos específicos

Os objetivos específicos deste projeto, que visa abordar a especificação CORS, são:

1. Detalhar o funcionamento teórico da especificação CORS, apresentando toda a mecânica envolvida no diálogo entre as aplicações envolvidas em uma comunicação cross-domain;
2. Desenvolver um estudo de caso para demonstrar a aplicabilidade prática do CORS. Este estudo de caso deverá abranger o desenvolvimento passo a passo de duas aplicações:
   * Aplicação api-provider, cuja finalidade será disponibilizar serviços RESTful consumíveis por diversas origens;
   * Aplicação api-consumer, cujo objetivo será fazer o consumo, via AJAX, dos serviços disponibilizados pela aplicação api-provider.
3. Informar a atual aderência dos principais navegadores web para com a especificação CORS, indicando quais características já se tornaram realidade e quais ainda são tendência.

## Relevância

Este projeto visa simplificar e melhorar a qualidade do desenvolvimento de aplicações que efetuem interações com aplicações externas as suas fronteiras de domínio utilizando o conceito de requisições assíncronas AJAX.

A simplificação deste desenvolvimento é dada através da minimização do esforço de configurações externas ao escopo da aplicação, como intervenções em Web Servers. A remoção desta dependência arquitetural é de grande valia em ambientes corporativos pois, como consequência, diminuímos os esforços delegados a área de infra-estrutura.

A forma semi transparente com que a solução apresentada é aplicada também torna os elementos participantes da comunicação cross-domain mais coesos, ou seja, eles não precisam saber nada além do que solicitar e do que responder. Toda negociação de acesso aos recursos fica apartada e abstraída, tornando o código do cliente e do servidor mais limpo. Isso maximiza a legibilidade do código e o seu nível de manutenabilidade.

Como resultado das vantagens apresentadas previamente, este projeto tem como finalidade contribuir com a disseminação de conhecimento da especificação CORS, proporcionando melhorias de qualidade do código, aumento na segurança das informações trafegadas e redução de complexidade e de recursos necessários para o desenvolvimento, como tempo e pessoas.

# REVISÃO BIBLIOGRÁFICA

## Contextualização

Capítulo 3

Introdução

Com a emergente demanda de compartilhamento de API’s públicas e privadas, surge a necessidade de criação um modelo mais robusto e padronizado de compartilhamento de dados entre origens dissemelhantes. possuindo que possua como características, a passível de ser utilizado assíncronamente, capaz de estender a política de mesma origem sem causar perdas no âmbito da segurança.

livros

[FLANAGAN, 2011] FLANAGAN, DAVID. **JavaScript: The Definitive Guide, 6a edição**. Sebastopol, USA: O’Reilly Media, 2011.

[PRATES, 2010] PRATES, RUBENS. **JavaScript: Guia do Programador, 1a edição**. São Paulo, BRA: Editora Novatec, 2010.

sites

[JSON-P, 2008] JSON-P: Safer cross-domain Ajax with JSON-P/JSONP. Disponível em: <http://json-p.org/>. Acesso em: Oububro de 2008.

Na introdução, contextualiza-se o objeto de estudo, tema e o problema de pesquisa, segundo o marco teórico que sustentará o desenvolvimento da pesquisa. Há que se esclarecer os limites para o seu desenvolvimento, a JUSTIFICATIVA da investigação por meio de uma REVISÃO BIBLIOGRÁFICA, em que se faz referência a estudos e pesquisas já realizados sobre o assunto em questão. O TEMA da pesquisa define o assunto a ser tratado e resulta da relação da área do conhecimento usada para resolver o problema associado ao objeto de estudo. Pode equivaler ou não ao título do projeto ou da pesquisa. Deve ter um significado preciso. Já o PROBLEMA deve ser ainda mais específico que o tema. Formulado como pergunta, deve ser associado ao marco teórico da investigação a ser feita e as demandas institucionais e sociais. Além disso, deve ser completo, ou seja, conter as variáveis necessárias e esclarecedoras da investigação.

A revisão bibliográfica, para justificar a pesquisa, pode ser feita, optando-se por um dos seguintes argumentos:

1) O pesquisador demonstra a análise incompleta ou insuficiente acerca do objeto de estudo.

2) Por meio da literatura selecionada, o estudioso demonstra contradições entre os autores em relação ao problema enunciado.

3) O estudioso deseja colocar em xeque as conclusões encontradas sobre o objeto de estudo.

4) O pesquisador necessita retestar os resultados já obtidos em outras investigações.

Os OBJETIVOS são as metas a serem alcançadas com a realização do trabalho, por meio de verbos no infinitivo, como: demonstrar, identificar, observar, analisar, comparar. A melhor forma de destacá-los é dividi-los em geral e específicos. O GERAL deve se referir ao produto que se deseja obter com a investigação. Já OBJETIVOS ESPECÍFICOS (devem conter, no mínimo, três) possuem natureza operacional, isto é, referem-se a procedimentos que deverão ser cumpridos para que o objetivo geral seja atingido, confirmando ou não a hipótese

**Organização do Trabalho**

A organização do trabalho é a descrição de como será dividido o trabalho, sendo opcional o uso de capítulos, porém, é mais comumente usado a divisão do trabalho em capítulos. A seguir segue um exemplo do texto da organização do trabalho:

O trabalho está dividido em oitos capítulos/partes, descritos resumidamente a seguir:

No capítulo I, são apresentados os conceitos e definições sobre...

# CAPITULO I

# REFERENCIAL TEÓRICO

## Introdução

Em todo capítulo a primeira seção deve ser a introdução que consiste num pequeno texto que apresenta o capítulo e antecipa o que será relatado.

## Referencial Teórico

Indica-se a fundamentação, o marco teórico, o estado da arte ou o estado do debate que orienta o estudo.[[1]](#footnote-1) Este referencial é considerado como um elemento de controle de toda a pesquisa, desde a problematização inicial. O pesquisador irá interpretar seu objeto de estudo de acordo com a concepção teórica de uma ou toda a obra de um autor ou de um conjunto de autores, ou seja, o marco previamente determinado. Nas áreas de Ciências Exatas, opta-se pela avaliação de um conjunto de produtos ou objetos desenvolvidos relacionados com o tema da pesquisa, chamado de Estado da Arte. Apresenta-se de modo aprofundado, respondendo quais os princípios, categorias, conceitos ou teorias fundamentam a pesquisa. Deve estar de acordo com a problemática formulada e o raciocínio desenvolvido nas fases anteriores. Cabe alertar que, caso o marco teórico seja mudado durante a pesquisa, todos os demais elementos, como problema, hipótese, objetivos (geral/específicos), caem por terra, o que significa que o estudo será outro e terá um novo começo.

Portanto o referencial teórico é toda a teoria que norteia o tema escolhido pelo pesquisador juntamente com determinação clara do marco teórico ou estado da arte.

### Subseções

O texto pode apresentar subseções até o terceiro nível como está no tópico acima. A partir daí sugere-se colocar outro mecanismo para dividir o texto, por exemplo as letras do alfabeto (a, b, c..).

## Figuras

Todo desenho, gráfico, imagem devem ser considerados em uma monografia como figura. As figuras devem sempre ser colocadas sempre abaixo da imagem, seguida de um texto que apresente a mesma. Uma figura não deve iniciar uma seção sem um texto precedente que a apresente e cite a figura. Toda vez que a figura é citada no texto, a mesma deve ser escrita com a inicial maiúscula (... como mostra a Figura 1).

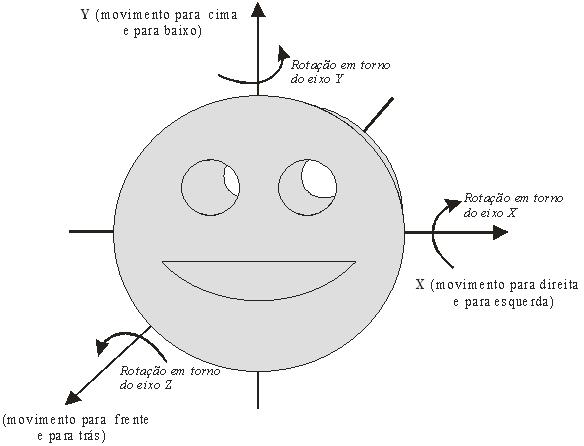


Figura 1. Exemplo de uma figura no texto. (RIBEIRO, 2006)

A Figura 1 apresenta um modelo de figura juntamente com sua descrição.

## Tabelas

As tabelas não podem ser confundidas com imagens, figuras ou similares, é uma construção própria do editor de textos, e, mesmo tabelas que foram construídas por outros aplicativos e são caracterizadas como imagem, devem ser consideradas figuras e não tabelas. As tabelas devem ter legendas na parte superior, e em alguns padrões não possuem bordas laterais e intermediárias.

# Tabela 1 – Tabela de formatos para monografia

|  |  |
| --- | --- |
| **Formatos** | **Características** |
| Tamanho do Papel | A4 (21 cm x 29,7 cm) |
| Margens | Esquerda e Superior = 3cm – Direita e Inferior = 2 cm |
| Tipo da Fonte | Times New Roman |
| Tamanho da Fonte | 12 para texto e 10 para citações com mais de três linhas |
| Títulos da Partes ou Capítulos | Centralizados e Negritos |
| Espaçamento | 1,5 linha e simples para citações com mais de três linhas |
| Notas de Rodapé | Tamanho 10 |
| Início das Partes ou Capítulos | Sem numeração e com título iniciando a oito (8) centímetros da margem |
| Contagem de folhas | Sequencialmente a partir da folha de rosto |
| Numeração | Em algarismos arábicos no canto superior direito, exceto nas páginas de início de capítulos. |

# CONCLUSÕES E TRABALHOS FUTUROS

## 2.1 Introdução

Este capítulo apresenta os principais tópicos discutidos nesse trabalho, relaciona os possíveis trabalhos futuros advindos dessa pesquisa e avalia a principal contribuição da mesma.

## 2.2 Conclusões

Na conclusão restabelecem-se os argumentos mais relevantes expostos no desenvolvimento do trabalho, a síntese-crítica dos resultados obtidos e a contribuição do estudo efetivado (se o estudo feito não esgotou o problema investigado, cabe apontar esses vazios e as possíveis formas de preenchê-lo).

## 2.3 Trabalhos Futuros

Na seção de Trabalhos Futuros, é necessário estabelecer os possíveis caminhos que não foram percorridos neste trabalho e também há, ainda, que se indicar as correções metodológicas em novas pesquisas semelhantes.

REFERÊNCIAS BIBLIOGRÁFICAS

Deve ser redigido em ordem alfabética, espaço simples entre linhas, e dois espaços simples para separar as próprias obras. Quando se tratar de obras de um mesmo autor, as quais aparecem sucessivamente, o nome deste deve ser substituído por um traço equivalente a seis espaços.

Exemplo:

RIBEIRO, Marcos Wagner de Souza. **Arquitetura para distribuição de ambientes virtuais multidisciplinares.** 2006. 178f. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Engenharia Elétrica, UFU, Uberlândia, 2006.

1. Como, por exemplo, a Teoria do Discurso de Jürgen Habermas, o materialismo histórico dialético de Karl Marx, o positivismo de August Comte, o enfoque experimental segundo a corrente de pensamento empirista, o estruturalismo conforme a obra de Claude Lévi-Strauss, entre outros. [↑](#footnote-ref-1)